Chapter 4

Return

In this chapter we will return to our introductory problem and get some glimpses from the field of number theory.

4.1 Reminiscence

The question from the beginning of the book, in a slightly elaborated version was to find a digit sequence `xyz…` such that:

```
A:     0.xyz........
B:     0.00xyz......   ( B=1% of A=10⁻²A )
C:     0.00000xyz...   ( C=1‰ of B=10⁻⁵A )
A+B+C=0.99999999...
```

This is easily solved by setting up the equation $A + 10^{-2}A + 10^{-5}A = 1$. The digit sequence is found by long division on $A = 10^5/(10^5 + 10^3 + 1)$. The procedure of long division shows that the decimal expansion of p/q is either finite or ends with a repeating digit sequence of length $\leq q - 1$. The division algorithm gives us `xyz…`$= \overline{990089207\ldots0099900000}$ with 16 640 digits in the repeating sequence. Elaborating a bit more:

$$A + B + C + D = 1 \quad \begin{matrix} B = 1\%\text{ of } A \\ C = 1\text{ppm of } B \\ D = 1‰\text{ of } C \end{matrix} \rightarrow \quad A = \frac{10^{2+6+3}}{10^{2+6+3} + 10^{6+3} + 10^3 + 1}$$

A is a fraction with a repeating sequence that is 25 014 018 913 digits long. With the simple probability model for decimal expansion on page 105 such long repeaters should not occur. A better model is needed to analyze periods of fractions. The repeating sequence and its length depends on the base of the expansion, it is not a property of the fraction itself. A better analysis should cover all bases, not just decimal expansions.

4.2 Reptends and Base

A good place to start is with terminology. The shortest repeating sequence at the end of an expansion is called **reptend**. The length of the reptend is called the **period**. Rational numbers, expressed in a certain base can be divided into those with a finite number of digits, called **terminating** or **regular** numbers

and those that ends with a repeating sequence that is not $\bar{0}$ or $\overline{b-1}$, (base b). These numbers have many names: **repeating**, **recurring**, **non-terminating** or **non-regular**. Terms used for numbers expanded in a selection of bases are binary-2, ternary-3, quaternary-4, quinary-5, senary-6, septenary-7, octal-8, nonary-9, decimal-10, undecimal-11, duodecimal-12, hexadecimal-16, vigesimal-20 and sexagesimal-60.

Theorem.

Every base b expansion of the form $z = \left(x_1 \dots x_i . y_1 \dots y_j \overline{r_1 \dots r_k}\right)_b \in \mathbb{Q}$
$i, j \in \{0,1, \dots\}, k \in \{1,2, \dots\}, b \in \{2,3, \dots\}, x_l, y_m, r_n \in \{0,1, \dots, b-1\}$

Proof.

$$b^j z = x_1 \dots x_i y_1 \dots y_j . \overline{r_1 \dots r_k} \qquad \left.\begin{matrix}(b^{j+k} - b^j)z \in \mathbb{Z} \\ b^{j+k} - b^j \in \mathbb{Z}^+\end{matrix}\right\} \Longrightarrow z \in \mathbb{Q} \qquad \blacksquare$$

The converse, every rational has the form above follows from long division. The reptend is the first appearance of the repeating part in the expansion, its preceding digit must differ from r_k and it has no repeating subpart but it may straddle the decimal point, or rather the **radix point**, a name for all bases. The sequence $y_1 .. y_j$ after radix point and before reptend is called **transient**.

When going in the other direction, finding reptends and periods of a rational number it will always be assumed, even if not stated that m/n is in reduced form $(m, n) = 1$, no common factors, m and n are **relatively prime** a.k.a. **co-prime**. The x-part is not very interesting, if $z = m/n$ it is just $\lfloor m/n \rfloor$ so from now on we will assume $m \in \{1,2, \dots, n-1\}$ and $z = (0. y\bar{r})_b$.

Theorem.

m/n is terminating in base $b \Leftrightarrow n$ has no prime factors other than those in b

Proof.

$$\Rightarrow \left.\begin{matrix}m/n \text{ is terminating} \\ (m, n) = 1\end{matrix}\right\} \Rightarrow \exists N: b^N \cdot \frac{m}{n} \in \mathbb{Z} \Rightarrow n | b^N \Rightarrow \begin{cases}n \text{ has no factors} \\ \text{other than } b's\end{cases}$$

$$\Leftarrow \left.\begin{matrix}n = \prod_{i=1}^{k} {b_i}^{a_i} \\ b_i | b\end{matrix}\right\} \Rightarrow \frac{m}{n} \cdot \underbrace{b^{a_1 + \dots + a_k}}_{\text{moves radix point}} = m \left(\frac{b}{b_1}\right)^{a_1} \cdot \dots \cdot \left(\frac{b}{b_k}\right)^{a_k} \in \mathbb{Z} \Longrightarrow$$

m/n is a terminating number in base b. $\blacksquare$

For base 2 the only regular numbers are $m/2^k$ and for base 10, $m/(2^a 5^b)$.

Theorem.
The number of decimals in $1/(2^a 5^b)$ is $\max(a, b)$.

Proof.
$1/(2^a 5^b) = 0.d_1 \dots d_N \Rightarrow N = \min\{k \in \mathbb{Z}^+ | z \cdot 10^k \in \mathbb{Z}\}$
$\left.\begin{matrix} z \cdot 10^{\max(a,b)} \in \mathbb{Z} \\ z \cdot 10^{\max(a,b)-1} \notin \mathbb{Z} \end{matrix}\right\} \Longrightarrow N = \max(a, b)$ ■

The natural counterpart for base $b = \prod_{i=1}^{N} b_i^{k_i}$ with primes b_i is:
$z = (\prod_{i=1}^{N} b_i^{k_i})^{-1}$ with $k \in \mathbb{N}_0$ has $\max\limits_{1 \le i \le N}(k_i)$ digits after the radix point.
There is no transient when the denominator is coprime with the base.

Theorem.
$z = \frac{m}{n} = (0.\overline{r_1 \dots r_k})_b \Leftrightarrow (n, b) = 1 \qquad (m, n) = 1 \text{ and } 0 < m < n$

Proof.
$\Rightarrow \ (b^k - 1)z = r_1 \dots r_k \Rightarrow z = \frac{r_1 \dots r_k}{b^k - 1} = \frac{m}{n} \quad (m, n) = 1$
$(b^k - 1, b) = 1 \text{ and } n | (b^k - 1) \Rightarrow (n, b) = 1$

$\Leftarrow$ is the same as showing:
$z = 0.\underbrace{y_1 \dots y_j}_{y}\,\underbrace{\overline{r_1 \dots r_k}}_{r}$ with $j, k \ge 1$ and $y_j \ne r_k \Longrightarrow z = m/n \wedge (n, b) \ne 1$
$b^{j+k} z - b^j z = y_1 \dots y_j r_1 \dots r_k - y_1 \dots y_j \rightarrow z = \frac{y b^k + r - y}{b^j (b^k - 1)}$
$y b^k + r - y \pmod b = r - y \pmod b = r_k - y_j \pmod b \ne 0 \Longrightarrow$
$z = m/n$ with $(n, b) \ne 1$ ■

$\therefore$ m/n has digits preceding the reptend iff n has some factor from the base.

The number of digits in the transient of m/n where $n = n' \cdot \prod_{i=1}^{N} b_i^{k_i}$ with $(n', b) = 1$ and $b_i | b$ is $\max\limits_{1 \le i \le N}(k_i)$.

In the rest of this chapter focus will be on the reptend and the number of digits in the reptend i.e. the period of m/n.

Theorem.
The period of m/n divides the period of $1/n$.
Regular number are assumed to have period one, with "reptend" 0 or $b - 1$.

Proof.

$1/n = 0.\underbrace{y_1 \ldots y_j}_{y}.\overline{\underbrace{r_1 \ldots r_k}_{r}} = yb^{-j} + r(b^{-(j+k)} + b^{-(j+2k)} + \cdots)$

$m/n = myb^{-j} + mr(b^{-(j+k)} + b^{-(j+2k)} + \cdots)$

If mr has more than k digits divide it into blocks of length k, starting from the right and add them repeatedly to get a sequence of k digits or less. Prepend the sequence with zeroes to get a repeating k-digit sequence. The repeating part may equal $\overline{b-1}$ which makes m/n regular or it may contain a repeating subsequence that makes the period of m/n a divisor of $1/n$. ■

Example.

$1/880 = 0.001\overline{136} = y + 36(10^{-6} + 10^{-8} + \cdots)$ Reptend=36 Period=2

$$\begin{aligned} 751/880 &= y_1 + 751 \cdot 36(10^{-6} + 10^{-8} + \cdots) \quad (y \text{ and } y_i \text{ are terminating}) \\ &= y_1 + \underbrace{27036}_{02+70+36}\ (10^{-6} + 10^{-8} + \cdots) \\ &= y_2 + \underbrace{108}_{01+08}\ (10^{-6} + 10^{-8} + \cdots) \\ &= y_3 + 09(10^{-6} + 10^{-8} + \cdots) \text{ Reptend=09 Period=2} \end{aligned}$$

A situation with a reptend of m/n dividing the reptend of $1/n$ would be if we got a situation $r_1 r_1$, a period one reptend or say if starting from period 6 with $\overline{r_1 \ldots r_6}$ and ending up with $\overline{r_1 r_2 r_1 r_2 r_1 r_2} = \overline{r_1 r_2}$ of period 2. A search for such examples will be futile.

Proof that the periods of m/n and $1/n$ are always equal will be given shortly or rather two proofs; one based on modular arithmetic and a second proof using group theory. With no need for numerators let T_n designate the period of $1/n$ in base 10 and let $T_n(b)$ be the period of $1/n$ in base b.

Factors from the base can be separated from the denominator and removed without affecting the period.

Theorem.

$T_n(b) = T_{n'}(b)$ if $n = n' \cdot b'$ where $\begin{matrix} n' \text{ has no factor of the base} \\ b' \text{ has only factors of the base} \end{matrix}$

Proof.

Extend numerator and denominator of $1/n$ with factors from the base to get a pure power of the base in the denominator.

$\dfrac{1}{n} = \dfrac{1}{n'b'} = \dfrac{b''}{n'b^k}$ b'' has no affect on the period and b^k only moves the radix point.

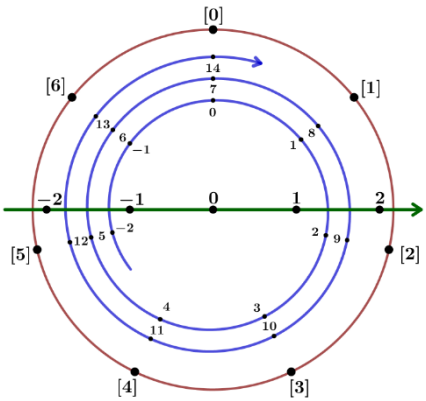
∴ The period of $1/n$ and $1/n'$ must be the same. ■

Expansion of $1/n$ in base 10 as $0.y_1 \dots y_j\overline{r_1 \dots r_k}$											
n	$y_1 \dots y_j$	$r_1 \dots r_k$	T_n	n	$y_1 \dots y_j$	$r_1 \dots r_k$	T_n	n	$y_1 \dots y_j$	$r_1 \dots r_k$	T_n
1	–	–	–	34	0	294..235	16	67	–	014..597	33
2	5	–	–	35	0	285714	6	68	01	470..176	16
3	–	3	1	36	02	7	1	69	–	014..971	22
4	25	–	–	37	–	027	3	70	0	142857	6
5	2	–	–	38	0	263..105	18	71	–	014..169	35
6	1	6	1	39	–	025641	6	72	013	8	1
7	–	142857	6	40	025	–	–	73	–	013..863	8
8	125	–	–	41	–	024390	6	74	0	135	3
9	–	1	1	42	0	238095	6	75	01	3	1
10	1	–	–	43	–	023..093	21	76	01	315..526	18
11	–	09	2	44	02	27	2	77	–	012987	6
12	08	3	1	45	0	2	1	78	0	128205	6
13	–	076923	6	46	0	217..565	22	79	–	012..481	13
14	0	714285	6	47	–	021..617	46	80	0125	–	–
15	0	6	1	48	0208	3	1	81	–	012..679	9
16	0625	–	–	49	–	020..551	42	82	0	12195	5
17	–	058..647	16	50	02	–	–	83	–	012..253	41
18	0	5	1	51	–	019..549	16	84	01	190476	6
19	–	052..421	18	52	01	923076	6	85	0	117..294	16
20	05	–	–	53	–	018..283	13	86	0	116..465	21
21	–	047619	6	54	0	185	3	87	–	011..977	28
22	0	45	2	55	0	18	2	88	011	36	2
23	–	043..913	22	56	017	857142	6	89	–	011..191	44
24	041	6	1	57	–	017..807	18	90	0	1	1
25	04	–	–	58	0	172..655	28	91	–	010989	6
26	0	384615	6	59	–	016..661	58	92	01	086..826	22
27	–	037	3	60	01	6	1	93	–	010..043	15
28	03	571428	6	61	–	016..459	60	94	0	106..085	46
29	–	034..931	28	62	0	161..645	15	95	0	105..842	18
30	0	3	1	63	–	015873	6	96	01041	6	1
31	–	032..129	15	64	015625	–	–	97	–	010..567	96
32	03125	–	–	65	0	153846	6	98	0	102..755	42
33	–	03	2	66	0	15	2	99	–	01	2

Fig. 4.1 Table of $0.y_1 \dots y_j\overline{r_1 \dots r_k}$ for $1/n$ with $n = 1,2, \dots ,99$.

If $n = 2^a 5^b n'$ with n' coprime to 10 then the number of digits in $y_1 \dots y_j$ equals $\max(a, b)$. If n only has factors from the base, $n' = 1$ and there will be no reptend. The period is unaffected by base factors $T_n = T_{n'}$. The period of $1/n$ is often referred to as the period of n.

4.3 Modular Arithmetic



The decimal part of m/n and $(m+kn)/n$ $(m,k \in \mathbb{N}_0, n \in \mathbb{N}_1)$ are identical. When we study fractions with denominator n we can regard m and $m+kn$ as the same object. If we expand the domain of m and k into $\mathbb{Z}$ nothing much happens. If m and $m+kn$ are of opposite sign, reptends and transients will be complementary with digits adding up to 9 (base - 1).

Ex: $183/700 = 0.26\overline{142857} \rightarrow (183 - 5 \cdot 700)/700 = -4.73\overline{857142}$).

It's always a good idea when dealing with a problem to strip away everything that doesn't matter and concentrate on what remains. In our case this means to partition the integers into classes based on the equivalence relation $a \sim b$ whenever $a - b$ is a multiple of n. The notation for this is $a \equiv b \pmod{n}$ where a and b are said to be congruent modulo n. The congruence classes are $[0], [1], \ldots, [n-1]$ where $[i]$ corresponds to $\{i + kn | k \in \mathbb{Z}\}$ and $[m]$ is represented by its rest upon division: $m = kn + r$. The congruence classes form a set denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/n$.

Carl Friedrich Gauss introduced congruence classes and their arithmetic in *"Disquisitiones Arithmeticae"* from 1801. The arithmetical properties are as follows: (Check it!)

If $a_1 \equiv b_1 \pmod{n}$, $a_2 \equiv b_2 \pmod{n}$ and $a \equiv b \pmod{n}$ then:

$a + k = b + k \pmod{n}$, $k \in \mathbb{Z}$	Compatibility with	translation
$ka \equiv kb \pmod{n}$, $k \in \mathbb{Z}$		scaling
$a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$		addition
$a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$		subtraction
$a^k \equiv b^k \pmod{n}$		exponentiation
$p(a) \equiv p(b) \pmod{n}$, $p(x) \in \mathbb{Z}[X]$		polynomials

For cancellation the following apply:

$a + k \equiv b + k \pmod{n}$, $k \in \mathbb{Z} \quad \Rightarrow a \equiv b \pmod{n}$
$ka \equiv kb \pmod{n}$ and $(k, n) = 1 \Rightarrow a \equiv b \pmod{n}$

A big difference between modular arithmetic and integer arithmetic is the existence of multiplicative inverses.

$ax \equiv 1 \pmod{n}$ has a unique solution (mod n) whenever $(a, n) = 1$.
The solution denoted by a^{-1} is called modular multiplicative inverse.
$ax \equiv b \pmod{n}$ is solved by $x = a^{-1}b \pmod{n}$ whenever $\gcd(a, n) = 1$.
From now on $\gcd(a, b)$ (Greatest Common Divisor) will be used instead of (a, b) to be consistent with lcm(a, b) used for Least Common Multiple.

Every member of $\mathbb{Z}/p\mathbb{Z}$ with prime modulus has an inverse which makes $\mathbb{Z}/p\mathbb{Z}$ a field (p. 97). The number of elements in $\mathbb{Z}/n\mathbb{Z}$ with multiplicative inverse is given by Euler's totient function $\varphi(n)$ which counts the number of positive integers coprime with n. $\varphi(p) = p$-1 when p is a prime number and $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $\gcd(m, n) = 1$.

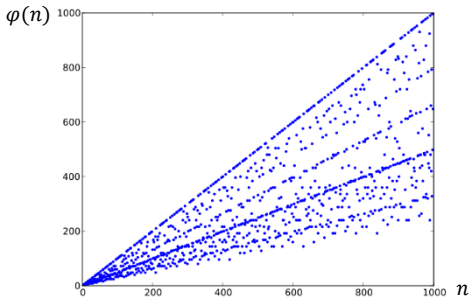


Fig 4.2 Euler's totient function $\varphi(n)$

Theorem. (Fermat's little theorem)
If p is a prime number: $a^p \equiv a \pmod{p}$
If $a \not\equiv 0 \pmod{n}$: $a^{p-1} \equiv 1 \pmod{p}$

Proof.
Assume $a \neq 0$ and $p \nmid a$:
$[a], [2a], \ldots, [(p-1)a]$ is a permutation of $[0], [1], \ldots, [p-1]$,
if not there would be a factor p in na with $0 < |n| < p$ and $p \nmid a$.
Their products must be identical modulo p:

$$\prod_{k=1}^{p-1} ka \equiv \prod_{k=1}^{p-1} k \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$$

If $a \equiv 0 \pmod{p}$ then $a^p \equiv a \equiv 0 \pmod{p}$. ■

Modular arithmetic has many applications not only problem solving in school mathematics. It's used in number theory, abstract algebra, computer science, cryptography and many other branches of science.

The Rivest-Shamir-Adleman cryptosystem

The RSA cryptosystem for encoding and decoding messages is based on choosing two large prime numbers p, q and computing the product $n = pq$ and $k = \varphi(n) = \varphi(p)\varphi(q)$. Two numbers e, d with $ed \equiv 1 \pmod{k}$ are used for encoding and decoding. n and the encryption key e are public while the decryption key d is private. A secret message represented by an integer m $(0 < m < n)$ is encrypted by computing $S = m^e \pmod{n}$ and decrypted by computing $M = S^d \pmod{n}$. Euler's theorem gives $M = m$. The RSA encryption would be useless if there was an easy method to factor n or if $\varphi(n)$ could be easily computed without factoring n.

From the expansion in base b of m/n with $0 < m < n$ and $\gcd(m, n) = 1$ with no transient, $m/n = (0.\overline{r_1 \dots r_k})_b$ it is quite obvious that the period of m/n is given by the smallest number k s.t.:

$$\underbrace{b^k \frac{m}{n} - \frac{m}{n}}_{r_1 \dots r_k} \in \mathbb{Z} \Leftrightarrow b^k m \equiv m \pmod{n} \Leftrightarrow b^k \equiv 1 \pmod{n}$$

This is the multiplicative order of b modulo n. $\gcd(b, n) = 1$ is assumed, this guarantees no transient. When there is a transient $m/n = \left(0.y_1 \dots y_j \overline{r_1 \dots r_k}\right)_b$ the transient length j and period k are given by the lowest pair (j, k) in lexicographic order s.t.:

$$\underbrace{b^{k+j} \frac{m}{n} - b^j \frac{m}{n}}_{y_1 \dots y_j r_1 \dots r_k} \in \mathbb{Z} \Leftrightarrow b^{k+j} \equiv b^j \pmod{n}$$

The period of a fraction m/n with no transient is most effectively calculated in Mathematica with the command `MultiplicativeOrder[b,n]`. This is much more efficient than the general procedure `RealDigits[m/n,b]` that gives $\{a_1, \dots, a_i, b_1, \dots, b_j, \{r_1, \dots, r_k\}, i\}$, with the period k given by the call `Length[RealDigits[m/n,b][[1,-1]]]`.

It remains to be seen whether the periods of $1/n$ and m/n are always equal.

To find out let's start by looking for counterexamples. This takes some programming but in order to take advantage of the commands available in Mathematica a good way would be to do the programming in Mathematica code. Debugging and code editing can be done in the Eclipse based IDE with a plug-in for the Mathematica language. Other plug-ins are available for other program languages such as C/C++, Java or Python.

```
countExceptions[nMax_,bMax_]:=
 Module[{countExc=0,countAll=0,periodOne,periodM},
  Do[                                          (* {b,2,bMax} *)
   Do[                                         (* {n,2,nMax} *)
    periodOne=Length[RealDigits[1/n,b][[1,-1]]];
    If[periodOne>0,                           (* ? 1/n repeat *)
     Do[                                      (* {m,2,n-1} *)
      If[ GCD[m,n]==1,
       periodM= Length[RealDigits[m/n,b][[1,-1]]];
       countAll=countAll+1;
       If[!(periodM==periodOne),countExc=countExc+1];
       ],                                     (* end If gcd=1 *)
      {m,2,n-1}
      ]                                       (* end Do m *)
     ],                                       (* end If p1>0 *)
    {n,2,nMax}
    ],                                        (* end Do n *)
   {b,2,bMax}
   ];                                         (* end Do b *)
  countExceptions=count;
  Print["Out of "<>ToString[countAll]<>" cases examined, "
        "the number of exceptions is "<>ToString[countExc]]
  ]                                           (* end Module *)
```

Running the program with countExceptions[nMax,bMax] gives no sign of exceptions because there are no exceptions.

Theorem.
The period of m/n equals the period of $1/n$. (if $\gcd(m,n) = 1$)

Proof.
The proof will be illustrated with concrete examples. A general proof will follow from the same principles as shown in the examples.

The remainder r when dividing a by n, $a = kn + r$ with $0 \le r < n$ will be $R_n(a) \equiv r = a - \lfloor a/n \rfloor \cdot n$ (it works for $a < 0$ as well).
In terms of congruence classes modulo n, $[a] = [R_n(a)]$.

$1/n = 0.y_1 \dots y_j\overline{r_1 \dots r_k}$ (Assume base 10)

The number of fractions m/n with $1 \le m < n$ and $\gcd(m,n) = 1$ is $\phi(n)$.
Collect them in the set $\Phi_n = \{k | 1 \le k < n \text{ and } \gcd(k,n) = 1\}$.
Ex.: $\Phi_{10} = \{1,3,7\}, \Phi_{13} = \{1,2,3,\dots,12\}$

Case 1. $1/n$ has no transient, i.e. $\gcd(n,10) = 1$ and $n^{-1} = 0.\overline{r_1 \dots r_k}$

Ex.: $1/13 = 0.\overline{076923}$, $T_{13} = 6$ is the smallest $x \in \mathbb{Z}^+ : 10^x \equiv 1 \pmod{13}$

With a convention of reptend always coming after the radix point $10^k/n$ will have a cyclically permuted reptend shifted k steps to the right and returning to the original reptend after T_n steps. The numerators 10^k will correspond to T_n different numerators $S_1 = (R_n(m_1 10^k))_{k=0}^{T_n-1}$.

Ex.: $n = 13$, $(m_1 = 1,10,10^2,10^3,\dots) \curvearrowright S_1 = (1,10,9,12,3,4,1,10,9,\dots)$

If not different then $10^a \equiv 10^b \pmod{n}$ and since $\gcd(10,n) = 1$ we get $10^{|b-a|} \equiv 1 \pmod{n}$ and with $0 < |b-a| < T_n$ this is a contradiction.

Take the next number in Φ_n not in S_1 and start a new sequence.
Ex. $m_2 = 2 \quad 2/13 = 0.\overline{153846} \quad (m_2 \cdot 10^k)_{k=1}^{\infty} \curvearrowright S_2 = (2,7,5,11,6,8)$

S_2 will also contain T_n different element before starting to repeat and each corresponding fraction will have the same period as $1/n$ since:
$m_2 \cdot 10^a \equiv m_2 \cdot 10^b \pmod{n} \underset{\substack{\gcd(m_2,n)=1 \\ \gcd(n,10)=1}}{\Leftrightarrow} 10^{|b-a|} \equiv 1 \pmod{n}$
$m_2 \notin S_1$ guarantees that $S_1 \cap S_2 = \emptyset$ since, the opposite means that
$\exists a,b: m_1 10^a \equiv m_2 10^b \Rightarrow m_1 10^{a+1} \equiv m_2 10^{b+1} \rightarrow m_2 \in S_1$ (contradiction)

Take the next number in Φ_n not belonging to $S_1 \cup S_2$ and repeat the process. Eventually all numerators in Φ_n will be accounted for, all with period T_n.

The fractions m/n can be divided into $\varphi(n)/T_n$ groups with T_n members with reptends equal to T_n cyclical permutations.

Ex. $n = 13$, $\varphi(13) = 12$, $T_{13} = 6$
$\frac{1}{13} = .\overline{076923}$ $\frac{10}{13} = .\overline{769230}$ $\frac{9}{13} = .\overline{692307}$ $\frac{12}{13} = .\overline{923076}$ $\frac{3}{13} = .\overline{230769}$ $\frac{4}{13} = .\overline{307692}$
$\frac{2}{13} = .\overline{153846}$ $\frac{7}{13} = .\overline{538461}$ $\frac{5}{13} = .\overline{384615}$ $\frac{11}{13} = .\overline{846153}$ $\frac{6}{13} = .\overline{461538}$ $\frac{8}{13} = .\overline{615384}$

Case 2. $1/n$ has a transient, i.e. $\gcd(n,10) \neq 1$ and $n^{-1} = 0.y_1..y_j\overline{r_1 \dots r_k}$

Ex. $n = 260 = 2^2 \cdot 5 \cdot 13$ $\frac{1}{n} = .00\overline{384615}$ $\varphi(260) = \varphi(2^2)\varphi(5)\varphi(13) = 96$ $T_{260} = 6$
Let the number of digits in the transient of $1/n$ be U_n.

Start with $m_1 = 1$ and look at $10^k \cdot (m_1/n)$ corresponding to numerators $R_n(m_1 \cdot 10^k)$. After U_n steps the reptend will reach the position after the radix point and then comes cycles with T_n steps: $10^{U_n+T_n} \equiv 10^{U_n} \pmod n$. Each fraction $10^k/n$ has the period T_n, same as $1/n$. Form S_1 as before.

Ex: $n = 260$ $S_1 = (1,10,100,220,120,160,40,110,)$ All numerators with period T_n.

The numerators $R_n(m_1 \cdot 10^k)$ in the circular part are all different, if not:

$m_1 10^{U_n} 10^a \equiv m_1 10^{U_n} 10^b \pmod n$
$0 \le a < b < T_n$
$\Leftrightarrow$ $10^{U_n+a} \equiv 10^{U_n+b} \equiv 10^{U_n+a+(b-a)} \pmod n$
Transient length: $U_n + a$
Period $b-a, 0 < b-a < T_n$ contradiction

Take the next number m_2 in Φ_n not in S_1 and start a new sequence, S_2.

$10^{U_n+T_n} \equiv 10^{U_n} \pmod n \Rightarrow m_2 \cdot 10^{U_n+T_n} \equiv m_2 \cdot 10^{U_n} \pmod n \Rightarrow$ All numerators in S_2 have the period T_n

As before, the numerators in the circular part will be different.

Ex: $n = 260$ $m_2 = 3$ $S_2 = (3,30,40,140,100,220,120,160,)$
$m_3 = 7$ $S_3 = (7,70,180,240,60,80,20,200,)$

Take the next number in Φ_n not belonging to $S_1 \cup S_2$ and repeat the process. Eventually all numerators in Φ_n will be accounted for, all with period T_n. ■

As a corollary we get that the period of $1/n$ is unaffected by any prime factors from the base. Let $n = n'b'$ with all prime factors from the base in b' and the rest in n'. Extend to get a base power in the denominator:

$$\frac{1}{n'b'} = \frac{b''}{n'b^k} \sim \frac{b''}{n'} \ (\gcd(b'',n) = 1) \sim \frac{1}{n'} \quad (\sim \text{meaning same period as})$$

4.4 Period and Prime Powers

To understand the period of any fraction we now only need to understand the period of $1/n$, with no factors from the base in n. We know $T_n(b) < n-1$ and from the big size of a few examples, the remainders in the long division can hardly be random. A reasonable way forward is to look for a rule such as $T_{\alpha\beta} = f(T_\alpha, T_\beta)$ whenever α and β are coprime.

Theorem.
If α and β are coprime with no factors from the base then $T_{\alpha\beta} = \text{lcm}(T_\alpha, T_\beta)$ (All periods are taken in base b)

Proof.
$T_n = \min \underbrace{\{x \in \mathbb{Z}^+ | b^x \equiv 1 \pmod{n}\}}_{S_n}$ with $n = \alpha, \beta$ or $\alpha\beta$

$b^{T_\alpha} \equiv 1 \pmod{\alpha} \quad b^{T_\beta} \equiv 1 \pmod{\beta} \quad b^{T_{\alpha\beta}} \equiv 1 \pmod{\alpha\beta}$

Show I. $\text{lcm}(T_\alpha, T_\beta) \in S_{\alpha\beta}$
II. $x \in S_{\alpha\beta}$ i.e. $b^x \equiv 1 \pmod{\alpha\beta} \Rightarrow x \geq \text{lcm}(T_\alpha, T_\beta)$

I.
For every common multiple y of T_α and T_β:
$y = k_\alpha T_\alpha \wedge b^{T_\alpha} \equiv 1 \pmod{\alpha} \Rightarrow b^y - 1 \equiv (b^{T_\alpha})^{k_\alpha} - 1 \equiv 0 \pmod{\alpha}$
$y = k_\beta T_\beta \wedge b^{T_\beta} \equiv 1 \pmod{\beta} \Rightarrow b^y - 1 \equiv \left(b^{T_\beta}\right)^{k_\beta} - 1 \equiv 0 \pmod{\beta}$

$$\begin{matrix} b^y - 1 = k_1\alpha \\ b^y - 1 = k_2\beta \end{matrix} \Rightarrow b^y - 1 = k_3\alpha\beta \Rightarrow y \in S_{\alpha\beta} \Rightarrow \text{lcm}(T_\alpha, T_\beta) \in S_{\alpha\beta}$$

II.
$$b^x - 1 = k\alpha\beta \Rightarrow \begin{matrix} b^x - 1 = k_1\alpha \Rightarrow x \text{ multiple of } T_\alpha \\ b^x - 1 = k_2\beta \Rightarrow x \text{ multiple of } T_\beta \end{matrix} \Rightarrow x \geq \text{lcm}(T_\alpha, T_\beta)$$

$\therefore$ $\text{lcm}(T_a, T_b)$ is the least element in $S_{\alpha\beta}$ so $\text{lcm}\left(T_\alpha, T_\beta\right) = T_{\alpha\beta}$ ■

Corollary.
If the prime factorization of n is $p_1^{k_1} p_2^{k_2} \ldots p_N^{k_N}$ then:

$$T_n = \text{lcm}\left(T_{p_1^{k_1}}, T_{p_2{}^{k_2}}, \ldots, T_{p_N^{k_N}}\right)$$ All periods taken in base b and $T_{b_i^{k_i}} = 1$ for prime powers of the base.

The period function $f_b(n) \equiv T_n(b)$ is not the only function with the property $f\left(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}\right) = \text{lcm}\left(f\left(p_1^{\alpha_1}\right), f\left(p_2^{\alpha_2}\right), \ldots, f\left(p_N^{\alpha_N}\right)\right)$. The totient function of Euler has a close relative called the Carmichael function a.k.a. the reduced totient function with the same property.

Definition. (the Carmichael function)
$\lambda(n) \equiv \min\{m \in \mathbb{Z}^+ | b^m \equiv 1 \pmod{n}$ for every b coprime to $n\}$

Think of b in the definition as a base, we are only interested in bases coprime to n when considering the period of $1/n$. $b^m \equiv R_n(b)^m \pmod{n}$ so we need only look at bases in Φ_n, the set from Euler's totient function.

To best understand $\lambda(n)$, some group and ring theory is needed. $\mathbb{Z}/n\mathbb{Z}$ is a ring, a group under addition but under multiplication only elements coprime to n have inverses. For prime numbers, every element has a multiplicative inverse, $\mathbb{Z}/p\mathbb{Z}$ is a field. The elements of $\mathbb{Z}/n\mathbb{Z}$ with multiplicative inverse form the multiplicative group modulo n, $((\mathbb{Z}/n\mathbb{Z})^*,\cdot)$. The set $(\mathbb{Z}/n\mathbb{Z})^*$ is the same as Φ_n with $|\Phi_n| = \varphi(n)$ members.

Example.

$n = 15 \quad \Phi_{15} = \{1,2,4,7,8,11,13,14\} \quad \varphi(15) = 8$

b	condition on m	m	order of b	period of $1/15$
1	$1^m \equiv 1 \pmod{15}$	k	1	1 in bases $\equiv 1 \pmod{15}$
2	$2^m \equiv 1 \pmod{15}$	$4k$	4	4 in bases $\equiv 2 \pmod{15}$
4	$4^m \equiv 1 \pmod{15}$	$2k$	2	2 in bases $\equiv 4 \pmod{15}$
⋮	⋮	⋮	⋮	⋮
14	$14^m \equiv 1 \pmod{15}$	$2k$	2	2 in bases $\equiv 14 \pmod{15}$

$\lambda(n)$ is the least m belonging to all rows → $\lambda(n) = \text{lcm}\{\text{ord}(b)|b \in \Phi_n\}$
By group theory the order of any element in the group divides the cardinality of the group which is $\varphi(n)$ so $\lambda(n)|\varphi(n) \rightarrow T_n(b)|\lambda(n)|\varphi(n) \leq n-1$.

∴ The period of $1/n$ in base b is a divisor of $\lambda(n)$ which is a divisor of $\varphi(n)$ which is smaller than n and maximal when n is prime, $\varphi(p) = p-1$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8	12
$\lambda(n)$	1	1	2	2	4	2	6	2	6	4	10	2	12	6	4	4	16	6	18	4	6
$T_n(2)$	-	-	2	-	4	2	3	-	6	4	10	2	12	3	4	-	8	6	18	4	6
$T_n(3)$	-	1	-	2	4	1	6	2	-	4	5	2	3	6	4	4	16	1	18	4	6
$T_n(7)$	-	1	1	2	4	1	-	2	3	4	10	2	12	1	4	2	16	3	3	4	1
$T_n(10)$	-	-	1	-	-	1	6	-	1	-	2	1	6	6	1	-	16	1	18	-	6
$T_n(16)$	-	-	1	-	1	1	3	-	3	1	5	1	3	3	1	-	2	3	9	1	3

Fig. 4.3 Euler's function φ, Carmichael's function λ and some comparison periods.

From now on focus will be on $T_{p^k}(b)$, period of prime powers for different bases. On the next page are tables for such periods. The first pattern to notice is that $T_p(b)|(p-1)$. We will return to the factor $k = (p-1)/T_p(b)$ at the end of the chapter. A second pattern seems to be that $T_{p^k}(b) = T_p(b) \cdot p^{k-1}$, but this rule is not without exceptions.

Base 2:

p:	2	3	5	7	11	13	17	19	23	29
k=1	0	2	4	3	10	12	8	18	11	28
k=2	0	$2\cdot 3^1$	$4\cdot 5^1$	$3\cdot 7^1$	$10\cdot 11^1$	$12\cdot 13^1$	$8\cdot 17^1$	$18\cdot 19^1$	$11\cdot 23^1$	$28\cdot 29^1$
k=3	0	$2\cdot 3^2$	$4\cdot 5^2$	$3\cdot 7^2$	$10\cdot 11^2$	$12\cdot 13^2$	$8\cdot 17^2$	$18\cdot 19^2$	$11\cdot 23^2$	$28\cdot 29^2$
k=4	0	$2\cdot 3^3$	$4\cdot 5^3$	$3\cdot 7^3$	$10\cdot 11^3$	$12\cdot 13^3$	$8\cdot 17^3$	$18\cdot 19^3$	$11\cdot 23^3$	$28\cdot 29^3$

Base 3:

p:	2	3	5	7	11	13	17	19	23	29
k=1	1	0	4	6	5	3	16	18	11	28
k=2	2	0	$4\cdot 5^1$	$6\cdot 7^1$	5	$3\cdot 13^1$	$16\cdot 17^1$	$18\cdot 19^1$	$11\cdot 23^1$	$28\cdot 29^1$
k=3	2	0	$4\cdot 5^2$	$6\cdot 7^2$	$5\cdot 11^1$	$3\cdot 13^2$	$16\cdot 17^2$	$18\cdot 19^2$	$11\cdot 23^2$	$28\cdot 29^2$
k=4	4	0	$4\cdot 5^3$	$6\cdot 7^3$	$5\cdot 11^2$	$3\cdot 13^3$	$16\cdot 17^3$	$18\cdot 19^3$	$11\cdot 23^3$	$28\cdot 29^3$

Base 4:

p:	2	3	5	7	11	13	17	19	23	29
k=1	0	1	2	3	5	6	4	9	11	14
k=2	0	3^1	$2\cdot 5^1$	$3\cdot 7^1$	$5\cdot 11^1$	$6\cdot 13^1$	$4\cdot 17^1$	$9\cdot 19^1$	$11\cdot 23^1$	$14\cdot 29^1$
k=3	0	3^2	$2\cdot 5^2$	$3\cdot 7^2$	$5\cdot 11^2$	$6\cdot 13^2$	$4\cdot 17^2$	$9\cdot 19^2$	$11\cdot 23^2$	$14\cdot 29^2$
k=4	0	3^3	$2\cdot 5^3$	$3\cdot 7^3$	$5\cdot 11^3$	$6\cdot 13^3$	$4\cdot 17^3$	$9\cdot 19^3$	$11\cdot 23^3$	$14\cdot 29^3$

Base 5:

p:	2	3	5	7	11	13	17	19	23	29
k=1	1	2	0	6	5	4	16	9	22	14
k=2	1	$2\cdot 3^1$	0	$6\cdot 7^1$	$5\cdot 11^1$	$4\cdot 13^1$	$16\cdot 17^1$	$9\cdot 19^1$	$22\cdot 23^1$	$14\cdot 29^1$
k=3	2	$2\cdot 3^2$	0	$6\cdot 7^2$	$5\cdot 11^2$	$4\cdot 13^2$	$16\cdot 17^2$	$9\cdot 19^2$	$22\cdot 23^2$	$14\cdot 29^2$
k=4	4	$2\cdot 3^3$	0	$6\cdot 7^3$	$5\cdot 11^3$	$4\cdot 13^3$	$16\cdot 17^3$	$9\cdot 19^3$	$22\cdot 23^3$	$14\cdot 29^3$

Base 6:

p:	2	3	5	7	11	13	17	19	23	29
k=1	0	0	1	2	10	12	16	9	11	14
k=2	0	0	5^1	$2\cdot 7^1$	$10\cdot 11^1$	$12\cdot 13^1$	$16\cdot 17^1$	$9\cdot 19^1$	$11\cdot 23^1$	$14\cdot 29^1$
k=3	0	0	5^2	$2\cdot 7^2$	$10\cdot 11^2$	$12\cdot 13^2$	$16\cdot 17^2$	$9\cdot 19^2$	$11\cdot 23^2$	$14\cdot 29^2$
k=4	0	0	5^3	$2\cdot 7^3$	$10\cdot 11^3$	$12\cdot 13^3$	$16\cdot 17^3$	$9\cdot 19^3$	$11\cdot 23^3$	$14\cdot 29^3$

Base 7:

p:	2	3	5	7	11	13	17	19	23	29
k=1	1	1	4	0	10	12	16	3	22	7
k=2	2	3^1	4	0	$10\cdot 11^1$	$12\cdot 13^1$	$16\cdot 17^1$	$3\cdot 19^1$	$22\cdot 23^1$	$7\cdot 29^1$
k=3	2	3^2	$4\cdot 5^1$	0	$10\cdot 11^2$	$12\cdot 13^2$	$16\cdot 17^2$	$3\cdot 19^2$	$22\cdot 23^2$	$7\cdot 29^2$
k=4	2	3^3	$4\cdot 5^2$	0	$10\cdot 11^3$	$12\cdot 13^3$	$16\cdot 17^3$	$3\cdot 19^3$	$22\cdot 23^3$	$7\cdot 29^3$

Base 8:

p:	2	3	5	7	11	13	17	19	23	29
k=1	0	2	4	1	10	4	8	6	11	28
k=2	0	2	$4\cdot 5^1$	7^1	$10\cdot 11^1$	$4\cdot 13^1$	$8\cdot 17^1$	$6\cdot 19^1$	$11\cdot 23^1$	$28\cdot 29^1$
k=3	0	$2\cdot 3^1$	$4\cdot 5^2$	7^2	$10\cdot 11^2$	$4\cdot 13^2$	$8\cdot 17^2$	$6\cdot 19^2$	$11\cdot 23^2$	$28\cdot 29^2$
k=4	0	$2\cdot 3^2$	$4\cdot 5^3$	7^3	$10\cdot 11^3$	$4\cdot 13^3$	$8\cdot 17^3$	$6\cdot 19^3$	$11\cdot 23^3$	$28\cdot 29^3$

Fig. 4.4 $T_{p^k}(b)$ for the first 10 primes, k=1 to 4 in base 2 to 8.

Exceptions to the rule $T_{p^k}(b) = T_p(b) \cdot p^{k-1}$ are marked with colors.

4.5 Exceptional Cases

Four cases deserve special study, the rest follows $T_{p^k}(b) = T_p(b) \cdot p^{k-1}$:

- Green: p is a factor of b then $1/p^k$ is a terminating number.
- Blue: $p = 2$ and the base b is an odd number.
- Orange: p is a factor of $b - 1$, $T_p(b) = 1$.
- Red: Special cases, not covered by the any of the above.

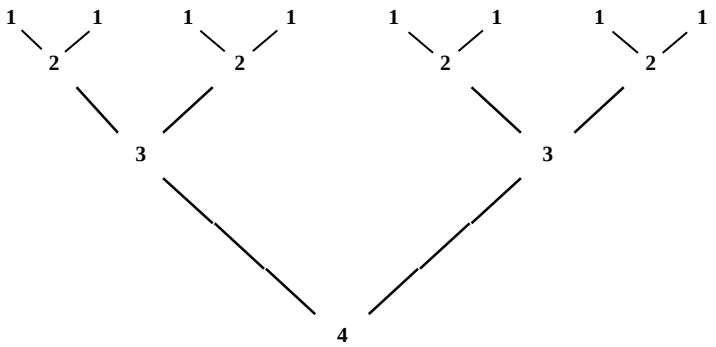
The first case we have already proved. The second case is $T_{2^k}(b)$ with odd b:

$T_{2^k}(b)$	k →	1	2	3	4	5	6	7	8	9	10		
b ↓	N ↓	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{64}$	$\frac{1}{128}$	$\frac{1}{256}$	$\frac{1}{512}$	$\frac{1}{1024}$	# 1's	# 2's
3	1	1	2	2	4	8	16	32	64	128	256	1	2
5	2	1	1	2	4	8	16	32	64	128	256	2	1
7	1	1	2	2	2	4	8	16	32	64	128	1	3
9	3	1	1	1	2	4	8	16	32	64	128	3	1
11	1	1	2	2	4	8	16	32	64	128	256	1	2
13	2	1	1	2	4	8	16	32	64	128	256	2	1
15	1	1	2	2	2	2	4	8	16	32	64	1	4
17	4	1	1	1	1	2	4	8	16	32	64	4	1
19	1	1	2	2	4	8	16	32	64	128	256	1	2
21	2	1	1	2	4	8	16	32	64	128	256	2	1
23	1	1	2	2	2	4	8	16	32	64	128	1	3
25	3	1	1	1	2	4	8	16	32	54	128	3	1
27	1	1	2	2	4	8	16	32	64	128	256	1	2
29	2	1	1	2	4	8	16	32	64	128	256	2	1
31	1	1	2	2	2	2	2	4	8	16	32	1	5
33	5	1	1	1	1	1	2	4	8	16	32	5	1
35	1	1	2	2	4	8	16	32	64	128	256	1	2
37	2	1	1	2	4	8	16	32	64	128	256	2	1
39	1	1	2	2	2	4	8	16	32	64	128	1	3
41	3	1	1	1	2	4	8	16	32	64	128	3	1
43	1	1	2	2	4	8	16	32	64	128	256	1	2
45	2	1	1	2	4	8	16	32	64	128	256	2	1
47	1	1	2	2	2	2	4	8	16	32	64	1	4
49	4	1	1	1	1	2	4	8	16	32	64	4	1
51	1	1	2	2	4	8	16	32	64	128	256	1	2
53	2	1	1	2	4	8	16	32	64	128	256	2	1
55	1	1	2	2	2	4	8	16	32	64	128	1	3
57	3	1	1	1	2	4	8	16	32	64	128	3	1
59	1	1	2	2	4	8	16	32	64	128	256	1	2
61	2	1	1	2	4	8	16	32	64	128	256	2	1
63	1	1	2	2	2	2	2	2	4	8	16	1	6

Fig. 4.5 Table of MatrixForm[Table[MultiplicativeOrder[b,2^k],{b,3,63,2},{k,1,10}]].

The number of 1's and 2's in each row seems to follow a pattern:

#1's base:	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
#2's base:		3	5	7	9	11	13	15	17	19	21	23	25	27	29



Base:	**3**	**5**	**7**	**9**	**11**	**13**	**15**	**17**	**19**	**21**	**23**	**25**	**27**	**29**	**31**
$\#1s = x$	1	2	1	3	1	2	1	4	1	2	1	3	1	2	1
$\#2s = y$	2	1	3	1	2	1	4	1	2	1	3	1	2	1	5

Theorem. (Blue cases)
Each sequence $(T_{2^k}(b))_{k=1}^{\infty}$ with an odd numbered base starts with x 1's followed by y 2's followed by a geometric sequence $(4 \cdot 2^k)_{k=0}^{\infty}$.
If the base is written as $b = \alpha \cdot 2^N + 1$ with $\alpha \in 2\mathbb{Z} + 1$ then $x = N$ and y is shifted one step, if $b = \alpha \cdot 2^M - 1$ then $y = M$.

Proof.
1's: For each b-sequence $\left(T_{2^k}(b)\right)_{k=1}^{\infty}$, $T_{2^k}(b) = 1 \Leftrightarrow b \equiv 1 \pmod{2^k}$
$\alpha \cdot 2^N + 1 \equiv 1 \pmod{2^k} \Leftrightarrow N \geq k \Leftrightarrow$ Each sequence start with N 1's.

2's: $T_{2^k}(b) \leq 2 \Leftrightarrow b^2 \equiv 1 \pmod{2^k} \Leftrightarrow (b+1)(b-1) \equiv 0 \pmod{2^k}$
Add the powers of 2 in $(b+1)$ and $(b-1)$:

Base b:	3	5	7	9	11	13	15	17	19	21	23	25	…
$b-1 = \alpha \cdot 2^N \to N$:	1	2	1	3	1	2	1	4	1	2	1	3	…
$b+1 = \alpha \cdot 2^M \to M$:	2	1	3	1	2	1	4	1	2	1	3	1	…
Blue + Green, $M+N$:	3		4		3		5		3		4		…

Number of 2's $y = (N+M)\ (for\ T \leq 2) - N\ (for\ T = 1) = M$
M is the same pattern as N but shifted one step.

Geometric sequence:
$T_{2^n}(b)|\varphi(2^n) \wedge \varphi(2^n) = 2^{n-1} \Rightarrow T_{2^n}(b) \in \{2^k | k = 1,2,\dots,n-1\}$

$b^2 \equiv 1 \pmod{2^k} \Rightarrow b^4 \equiv 1 \pmod{2^{k+1}}$ since
$(b+1)(b-1) \equiv 0 \pmod{2^k} \Rightarrow$
$(b^4-1) = \underbrace{(b^2+1)}_{\alpha_1 \cdot 2}\underbrace{(b^2-1)}_{\alpha_2 \cdot 2^k} \equiv 0 \pmod{2^{k+1}} \quad [\alpha_1, \alpha_2 \in 2\mathbb{Z}+1]$
$\therefore T_{2^k}(b) \leq 2 \Rightarrow T_{2^{k+1}}(b) \leq 4 \rightarrow$ after the $2's$ in $\left(T_{2^k}(b)\right)_{k=1}^{\infty}$ comes a 4.

Assume $T_{2^{K+2}}(b) = 4$ [$b^4 \equiv 1 \pmod{2^{K+2}}$ and $b^2 \not\equiv 1 \pmod{2^{K+2}}$]
$T_{2^{K+n}}(b) = 2^n$ [$b^{2^n} \equiv 1 \pmod{2^{K+n}}$]

Show $T_{2^{K+n+1}}(b) = 2^{n+1}$

$b^{2^{n+1}} = \left(b^{2^n}\right)^2 = (\alpha \cdot 2^{K+n}+1)^2 \equiv 1 \pmod{2^{K+n+1}} \quad [\alpha, \alpha_i \in 2\mathbb{Z}+1].$

Show $b^{2^n} \not\equiv 1 \pmod{2^{K+n+1}}$ $\alpha_i \in 2\mathbb{Z}+1$
$b^{2^n}-1 = \underbrace{\left(b^{2^{n-1}}+1\right)}_{2\alpha_{n-1}}\underbrace{\left(b^{2^{n-2}}+1\right)}_{2\alpha_{n-2}} \cdot \dots \cdot \underbrace{\left(b^{2^2}+1\right)}_{2\alpha_2}\underbrace{(b^4-1)}_{\alpha_0 2^{K+2}}$
$= \alpha 2^{K+n} \rightarrow \quad b^{2^n} \equiv 1 \pmod{2^{K+n}}$ and $b^{2^n} \not\equiv 1 \pmod{2^{K+n+1}}$

$\therefore T_{2^{K+n}}(b) = 2^{K+n}$ for $n = 1,2,\dots$
Once the sequence of 2's stop follows a geometric sequence 4, 8, 16, … ■

The third exceptional case is marked by orange in the table of fig. 4.4. It consists of powers of odd primes that are factors of base−1. The periods of even prime powers $T_{2^k}(b)$ is already covered in the second exception. The "orange" sequences $(T_{p^k}(b))_{k=1}^{\infty}$ all start with $T_p(b) = 1$, we could call them odd period one primes. The table should have been a bit longer to show what makes them special, $b = 10 \rightarrow b-1 = 3^2 \rightarrow T_{3^k} = (1,1,3,3^2,3^3,\dots)$. The number of 1's equals the power of the odd prime factor of $b-1$.

$$\frac{1}{b-1} = \frac{1}{b} + \frac{1}{b^2} + \frac{1}{b^3} + \cdots$$

$$1/(b-1) = (0.\bar{1})_b \rightarrow T_{b-1}(b) = 1$$

$$b-1 = p_1^{k_1} p_2^{k_2} \cdot \dots \cdot p_N^{k_N}$$

$$1 = \operatorname{lcm}\left(T_{p_1^{k_1}}(b), \dots, T_{p_N^{k_N}}(b)\right) \rightarrow T_{p_j^{k_j}}(b) = 1$$

$3^2|(10-1)$ $\quad \frac{1}{3^1}=0.\overline{3}$ $\quad \frac{1}{3^2}=0.\overline{1}$ $\quad \frac{1}{3^3}=0.\overline{037}$ $\quad \frac{1}{3^4}=0.\overline{012345679}$

Theorem. (Orange cases)
The sequences $(T_{p^k}(b))_{k=1}^{\infty}$ with p an odd prime factor of $b-1$ starts with $T_{p^k}(b)=1$ for $k \le N$ where N is given by: $b-1=\alpha p^N$ and $\gcd(\alpha,p)=1$. The 1's are followed by a geometric sequence $T_{p^{N+m}}(b)=p^m$ for $m \in \mathbb{Z}^+$.

Proof.

$$\left.\begin{matrix} b-1=\alpha P^N \\ \gcd(\alpha,p)=1 \end{matrix}\right\} \Rightarrow \begin{matrix} b \equiv 1 \pmod{p^k} & k \le N \\ b \not\equiv 1 \pmod{p^k} & k > N \end{matrix} \Rightarrow \begin{matrix} T_{p^k}(b)=1 & \text{for } k \le N \\ T_{p^k}(b)>1 & \text{for } k > N \end{matrix}$$

$b=1+\alpha p^N \rightarrow$

$$b^{p^m}=(1+\alpha p^N)^{p^m}=\sum_{i=0}^{p^m}\binom{p^m}{i}\alpha^i p^{Ni}=1+\sum_{i=1}^{p^m}\binom{p^m}{i}\alpha^i p^{Ni}$$

$$=1+p^{N+m}\left(\alpha+\frac{\alpha^2}{p^m}\binom{p^m}{2}p^N+\cdots+\frac{\alpha^{p^m-1}}{p^m}\binom{p^m}{p^m-1}p^{(p^m-1)N}+\frac{\alpha^{p^m}}{p^m}\binom{p^m}{p^m}p^{p^mN}\right)$$

$$=1+p^{N+m}(\alpha+kp) \quad [m \ge 1, N \ge 1, k \in \mathbb{Z}]$$

$b^{p^m} \equiv 1 \pmod{p^{N+m}} \Rightarrow T_{p^{N+m}}(b)|p^m$

For $m=1$: $\begin{matrix} T_{p^{N+1}}(b)|p \\ T_{p^{N+1}}(b)>1 \end{matrix} \Rightarrow T_{p^{N+1}}(b)=p$

For $m \ge 2$:

$$b^{p^{m-1}}=1+p^{N+m-1}\left(\alpha+\frac{\alpha^2(p^{m-1}-1)}{2}p^N+\cdots+\alpha^{p^{m-1}}p^{(p^{m-1}N-(m-1))}\right)$$

$$=1+p^{N+m-1}(\alpha+kp) \quad [\alpha,k \in \mathbb{Z}, \gcd(\alpha,p)=1]$$

$b^{p^{m-1}} \not\equiv 1 \pmod{p^{N+m}} \Rightarrow T_{p^{N+m}}(b) \nmid p^{m-1}$

$$\begin{matrix} T_{p^{N+m}}(b) \nmid p^{m-1} \\ T_{p^{N+m}}(b)|p^m \end{matrix} \Rightarrow T_{p^{N+m}}(b)=p^m \qquad \blacksquare$$

The remaining exceptions to $T_{p^k}(b)=T_p(b)\cdot p^{k-1}$ in table 4.4 are marked in red. They all seem to follow $(T_{p^k}(b))_{k=1}^{\infty}=(\alpha,\alpha,\alpha p,\alpha p^2,\dots)$. A search for exceptions not belonging to previous cases for $p \le 99$ and $b \le 18$ gives:

base 3 $\quad p=11 \quad (T_{11^k}(3))_{k=1}^{\infty}: \quad 5 \quad 5 \quad 5\cdot 11 \quad 5\cdot 11^2 \quad \dots$
base 7 $\quad p=5 \quad (T_{5^k}(7))_{k=1}^{\infty}: \quad 4 \quad 4 \quad 4\cdot 5 \quad 4\cdot 5^2 \quad \dots$

base 8	$p = 3$	$(T_{3^k}(8))_{k=1}^{\infty}$:	2	2	$2 \cdot 3$	$2 \cdot 3^2$	...
base 9	$p = 11$	$(T_{11^k}(9))_{k=1}^{\infty}$:	5	5	$5 \cdot 11$	$5 \cdot 11^2$	...
base 11	$p = 71$	$(T_{71^k}(11))_{k=1}^{\infty}$:	70	70	$70 \cdot 71$	$70 \cdot 71^2$	...
base 14	$p = 29$	$(T_{29^k}(14))_{k=1}^{\infty}$:	28	28	$28 \cdot 29$	$29 \cdot 29^2$	...
base 17	$p = 3$	$(T_{3^k}(17))_{k=1}^{\infty}$:	2	2	$2 \cdot 3$	$2 \cdot 3^2$	...
base 18	$p = 5$	$(T_{5^k}(18))_{k=1}^{\infty}$:	4	4	$4 \cdot 5$	$4 \cdot 5^2$	...
base 18	$p = 7$	$(T_{7^k}(18))_{k=1}^{\infty}$:	3	3	3	$3 \cdot 7$	$3 \cdot 7^2$ ...
base 18	$p = 37$	$(T_{37^k}(18))_{k=1}^{\infty}$:	36	36	$36 \cdot 37$	$36 \cdot 37^2$	...
			⋮				

What makes these primes in these bases special and what about the exception to the exceptions, $p = 7$ in base 18 that starts with three identical numbers instead of two before a possible geometric series?

The property that singles out these primes is not obvious. Fermat's little theorem states that for every prime $p \nmid b$, $b^{p-1} \equiv 1 \pmod{p}$ which in terms of periods means that $T_p(b) | (p-1)$. In some rare cases $b^{p-1} \equiv 1 \pmod{p^2}$ [$T_{p^2}(b) | (p-1)$]. All examples given so far from case 3 have this property. For the exception to the exception, $p = 7$ in base 18, $b^{p-1} \equiv 1 \pmod{p^3}$.

Definition. (Wieferich primes)
A base-b Wieferich prime of order n ($n \geq 2$) is a prime p that satisfies:

$$b^{p-1} \equiv 1 \pmod{p^n} \text{ and } b^{p-1} \not\equiv 1 \pmod{p^{n+1}}$$

A Wieferich prime of order n satisfies $b^{p-1} \equiv 1 \pmod{p^k}$ for every $k \leq n$, since $p^n | (b^{p-1} - 1) \Rightarrow \forall k \leq n : p^k | (b^{p-1} - 1)$.

Wieferich primes less than 10^8 of order 2 for bases less than 26.			
b	p	b	p
2	1093, 3511	14	29, 353
3	11	15	29131
4	1093, 3511	16	1093, 3511
5	2, 20771, 40487, 53471161	17	3, 46021, 48947
6	66161, 534851, 3152573	18	5, 37, 331, 33923, 1284043
7	5, 491531	19	3, 13, 43, 137, 63061489
8	3, 1093, 3511	20	281, 46457, 9377747
9	11, 1006003	21	2
10	3, 487, 56598313	22	13, 673, 1595813
11	71	23	13, 2481757, 13703077
12	2693, 123653	24	5, 25633
13	2, 863, 1747591	25	20771, 40487, 53471161

Fig. 4.6 Base-b Wieferich primes of order 2.

Some base-b Wieferich primes p of order n higher than 2.	
n	(b,p)
3	(18,7) , (19,7) , (26,3) , (124,11)
4	(80,3) , (161,3) , (182,5)
5	(242,3)

Fig. 4.7 Base-b Wieferich primes of higher order.

Examples:

Order 3 b=124 p=11 $(T_{11^k}(124))_{k=1}^{\infty}$: 5 5 5 $5\cdot 11^1$ $5\cdot 11^2$ ⋯

Order 4 b=182 p=5 $(T_{5^k}(182))_{k=1}^{\infty}$: 4 4 4 4 $4\cdot 5^1$ $4\cdot 5^2$ ⋯

Order 5 b=242 p=3 $(T_{3^k}(242))_{k=1}^{\infty}$: 2 2 2 2 2 $2\cdot 3^1$ $2\cdot 3^2$ ⋯

Theorem. (Red cases)

If p is a base-b Wieferich prime of order n then $T_{p^k}(b) = T_p(b)$ for $k \le n$ and $T_{p^{n+m}}(b) = T_p(b)\cdot p^m$ for $m \in \mathbb{Z}^+$.

Proof.

I. Show for $k \le n$: $T_{p^k}(b) = T_p(b) = T$ i.e. $b^T \equiv 1 \pmod{p^k}$ and $b^t \not\equiv 1 \pmod{p^k}$ for t < T

$$T_p(b) = T \to \begin{matrix} T|\varphi(p) \to p-1 = k_0 T \text{ and } p \nmid k_0 \\ b^T - 1 = k_1 p \to b^{nT} - 1 = (b^T-1)(\dots) \to b^{nT} = Kp+1 \\ b^t \not\equiv 1 \pmod{p} \text{ for } t < T \end{matrix}$$

Wieferich condition→ $\forall k \le n$: $b^{p-1} \equiv 1 \pmod{p^k}$

$$b^{p-1} - 1 = b^{k_0 T} - 1 = (b^T-1)\left(b^{(k_0-1)T} + \dots + b^T + 1\right) \to$$
$$b^{p-1} - 1 = (b^T-1)(K'p + k_0)$$

$$\forall k \le n: p^k | (b^{p-1}-1) \wedge p \nmid (Kp+k_0) \Rightarrow p^k | (b^T-1) \Rightarrow b^T \equiv 1 (\mathrm{mod}\ p^k)$$

$b^t \equiv 1 \pmod{p^k}$ for $t < T \Rightarrow b^t - 1 = Kp^k \Rightarrow b^t - 1 = K'p \Rightarrow$
$b^t \equiv 1 \pmod{p}$ for $t < T$, a contradiction to $T_p(b) = T$
$\therefore T_{p^k}(b) = T_p(b)$ for $k \le n$

II. Show $T_{p^{n+m}}(b) = T\cdot p^m$ for $m \in \mathbb{Z}^+$

A. Show $T_{p^{n+1}}(b) = T\cdot p$

$$b^{Tp} - 1 = (b^T-1)(b^{(p-1)T} + \dots + b^T + 1) \qquad [\, b^{\alpha T} = \beta p + 1 \,]$$
$$= (b^T-1)(kp+p)$$
$$T_{p^n}(b) = T \to b^T - 1 = k' p^n$$
$$b^{Tp} - 1 = k'' p^{n+1} \Rightarrow b^{Tp} \equiv 1 \pmod{p^{n+1}}$$

Assume $b^t \equiv 1 \pmod{p^{n+1}}$ with $t|Tp$ and $t < Tp$:

- $t < T \Rightarrow b^t \equiv 1 \pmod{p^n}$ contradicts $T_{p^n}(b) = T$
- $t = T \Rightarrow b^T \equiv 1 \pmod{p^{n+1}} \wedge b^{p-1} - 1 = (b^T - 1)(K'p + k_0) \Rightarrow$
  $b^{p-1} \equiv 1 \pmod{p^{n-1}}$ contradicts p being a Wieferich prime of order n
- $\begin{cases} t = \alpha p \\ \alpha | T, \alpha < T \end{cases} \rightarrow \begin{matrix} b^{\alpha p} \equiv 1 \pmod{p^{n+1}} \rightarrow b^{\alpha p} \equiv 1 \pmod{p^n} \\ p \text{ Wprime of order } n\text{: } \ b^{p-1} \equiv 1 \pmod{p^n} \end{matrix} \rightarrow (p-1)|\alpha p$
  $\rightarrow (p-1)|\alpha|T|(p-1) \rightarrow \alpha = T = (p-1) \rightarrow t = Tp$ a contradiction.

$\therefore b^t \not\equiv 1 \pmod{p^{n+1}}$ so $T_{p^{n+1}}(b) = Tp$

B. Prove by induction that $T_{p^{n+m}}(b) = T \cdot p^m$ for $m \in \mathbb{Z}^+$

$b^{Tp^m} - 1 = \left(b^{Tp^{m-1})}\right)^p - 1 = (kp^{n+m-1} + 1)^p - 1 = k'p^{n+m} \Rightarrow$
$b^{Tp^m} \equiv 1 \pmod{p^{n+m}} \Rightarrow T_{p^{n+m}}(b)|Tp^m$

Show $t < Tp^m \Rightarrow b^t \not\equiv 1 \pmod{p^{n+m}}$ Need only check $t < Tp^m$, $t|(Tp^m)$

Assume $t|Tp^{m-1}$ and $t < Tp^{m-1}$, If $b^t \equiv 1 \pmod{p^{n+m}}$ then
$b^t \equiv 1 \pmod{p^{n+m-1}}$ which contradicts $T_{p^{n+m-1}}(b) = Tp^{m-1}$.

Left to check is that $b^t \not\equiv 1 \pmod{p^{n+m}}$ when $t = Tp^{m-1}$.
$b^{Tp^{m-1}} - 1 = \left(b^{Tp^{m-2}}\right)^p - 1 =$
$\left(b^{Tp^{m-2}} - 1\right)\left(b^{(p-1)Tp^{m-2}} + b^{(p-2)Tp^{m-2}} + \cdots + b^{Tp^{m-2}} + 1\right) =$
$(Kp^{n+m-2})((kp^{n+m-2} + 1)^{p-1} + (kp^{n+m-2} + 1)^{p-2} + \cdots + (kp^{n+m-2} + 1) + 1) =$
$Kp^{n+m-2}\left(K'p^{n+m-2} + p^{n+m-2}\left((p-1)k + (p-2)k + \cdots + k\right) + p\right) =$
$Kp^{n+m-1}(K''p + 1) \wedge K \notin p\mathbb{Z} \Rightarrow$
$p^{n+m} \nmid \left(b^{Tp^{m-1}} - 1\right) \Rightarrow b^{Tp^{m-1}} \not\equiv 1 \pmod{p^{n+m}}$

$\therefore b^t \not\equiv 1 \pmod{p^{n+m}}$ for every $t < Tp^m$ and $b^{Tp^m} \equiv 1 \pmod{p^{n+m}}$

$\therefore \ T_{p^k}(b) = T_p(b)$ for $k \leq n$ and $T_{p^{n+m}}(b) = T_p(b) \cdot p^m$ for $m \in \mathbb{Z}^+$ ■

Wieferich primes of base 2, $p^2|(2^{p-1} - 1)$ were first considered by Arthur Wieferich (1884 – 1954) in connection with Fermat's last theorem. Only two such primes are known, 1093 and 3511. He proved that if $x^p + y^p + z^p = 0$ with p a prime such that $p \nmid xyz$ then p is a Wieferich prime (of base 2).

Very little is known about the distribution of these primes. A conjecture says that there is an infinite number of them for every order in each base and that the number of Wieferich primes below n is about $\log(\log(n))$. It would seem obvious that the number of non-Wieferich primes should be infinite but even this is hard to prove. It would follow from a proof of the abc conjecture.

The ABC conjecture and Shinichi Mochizuki

The abc conjecture is one of the most famous conjectures in mathematics. A long list of historic problems and conjectures would be solved by a proof of the abc conjecture. It was first proposed by Joseph Oesterlé and David Masserin the 1980's, the conjecture is also known as the Oesterlé-Masser conjecture. Some theorems following from the abc conjecture and unproved at the time have since been proved by other means.

Henceforth assume that $a, b, c \in \mathbb{Z}^+$ with $\gcd(a, b, c) = 1$ and $a + b = c$.

There is no obvious reason that links the prime factors of a and b to those of their sum c. The abc conjecture provides a link. It roughly states that if a and b have many small prime factors then c will have few and large prime factors. It can be stated in terms of the radical $\mathrm{rad}(n)$, a measure of the size of the primes in n, $\mathrm{rad}\left(p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}\right) \equiv p_1 p_2 \cdot \ldots \cdot p_n$. In most cases $\mathrm{rad}(abc) > c$. The abc conjecture is about the exceptions, how frequent and how extreme can they be. In terms of triples (a, b, c):

ABC conjecture: For every $\varepsilon > 0$ there is only finitely many (a, b, c) s.t.

$$\mathrm{rad}(a, b, c)^{1+\varepsilon} < c$$

$\varepsilon > 0$ is necessary, there are infinitely many triples with $\mathrm{rad}(abc) < c$:

Example.

$a = 1 \quad b = 2^{6n} - 1 = 64^n - 1 = (64 - 1)M = 9N \quad c = 2^{6n}$

$\mathrm{rad}(abc) = \mathrm{rad}(a)\mathrm{rad}(b)\mathrm{rad}(c) = 2 \cdot 3 \cdot \mathrm{rad}(b/9) \leq 2b/3 < 2c/3$

Each $n \in \mathbb{Z}^+$ gives an example where $\mathrm{rad}(abc) < c$. There is even an infinity of triples (a, b, c) with $\mathrm{rad}(a, b, c) < kc$ for any $k > 0$.

$a = 1 \quad b = 2^{p(p-1)n} - 1 \quad c = 2^{p(p-1)n}$ where p is an odd prime leads to $\mathrm{rad}(abc) < 2c/p$

Another way of formulating the abc conjecture is in terms of quality. The quality of a triplet (a, b, c) is defined as:

$$q(a, b, c) \stackrel{\text{def}}{=} \frac{\log(c)}{\log\left(\mathrm{rad}(abc)\right)} \quad \left(\mathrm{rad}(abc)^{q(a,b,c)} = c \right)$$

ABC conjecture: For every $\varepsilon > 0$ there is only finitely many (a, b, c) s.t.

$$q(a, b, c) > 1 + \varepsilon$$

There are infinitely many triples with $q(a, b, c) > 1$ but for any $\varepsilon > 0$ only a finite number of them has $q(a, b, c) > 1 + \varepsilon$. Assuming the abc conjecture true there should be a triple (a, b, c) that achieves the maximal possible value of $q(a, b, c)$. The highest quality found so far is 1.63:

$$\begin{array}{ll} a = 2 & \mathrm{rad}(abc) = 15042 \\ b = 3^{10} \cdot 109 = 6\,436\,341 \rightarrow & q(a, b, c) = 1.63\ldots \\ c = 23^5 = 6\,435\,343 & 15042^{1+0.63\ldots} = c \end{array}$$

Constructing a proof of the abc conjecture would give a proof of the statements listed below. Some of them have been proved later by other means, but a proof of ABC would still give new insights to the theorems.

- Roth's theorem, concerning how well irrational algebraic numbers are approximated by rational numbers:
  $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$ has only finitely many coprime solutions (p, q).
- Existence of infinitely many non-Wieferich primes in every base.
- Brocard's problem: find $(m, n) \in \mathbb{Z}^2$: $n! + 1 = m^2$. ABC implies that $n! + k = m^2$ has only finitely many solutions for any $k \in \mathbb{Z}$.
- Mordell's conjecture, important conjecture made by Mordell in 1922. A curve of genus > 1 over $\mathbb{Q}$ has only finitely many rational points. It was proved by Gerd Falting in 1983 and renamed Falting's theorem.
- Hall's conjecture in weak form for the distance between $y^2$and x^3:
  $\forall \varepsilon > 0\ \exists C > 0 : |y^2 - x^3| > C x^{1/2-\varepsilon} \quad (x, y) \in \mathbb{Z}^2$
  $\varepsilon = 0$ gives the original (strong) form, which is believed to be false.
- Fermat-Catalan's conjecture: $a^m + b^n = c^k$ with integer variables, $m, n, k > 0$, $1/m + 1/n + 1/k < 1$, distinct triplets (a^m, b^n, c^k) and $\gcd(a, b, c) = 1$ has only a finite number of solutions.
  Only ten are known and $1^m + 2^3 = 3^2$ is the only one with a 1 in it.
- The number of integer solutions to $y^m = x^n + k$ is finite. $(m, n > 1)$
- The number of integer solutions to $Ax^n - By^m = C$ with fixed positive integers A, B, C and $(m, n) \neq (2,2)$ is finite.
- Bael's conjecture: If a, b, c, x, y and z are positive integers with $a^x + b^y = c^z$ and $x, y, z > 2$ then $\gcd(a, b, c) = 1$.
- Szpiro's modified conjecture for elliptic curves.

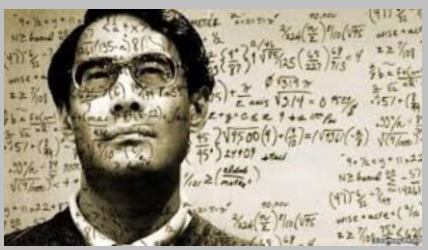
Fermat's last theorem, $a^n + b^n = c^n$ for $n \geq 6$ follows immediately if $q(a, b, c) \leq 2$ is assumed. The value for the upper limit of the quality $q(a, b, c)$ is however not a part of the abc conjecture.

Noam Elkie was one of the first to realize how a proof of abc conjecture would revolutionize the study of Diophantine equations (integer solutions to polynomial equations). He proved that abc would lead to solutions of a big collection of famous and unsolved equations. This is due to the explicit bounds that the conjecture sets on the size of a solution. To find all solutions, only numbers below that bound need to be considered.

This meant that the abc conjecture (if proved) would supersede Louis Mordell's conjecture from 1922 as the most important breakthrough in the history of Diophantine equations. Mordell's conjecture states that a curve of genus greater than 1 (more than two holes in it) with coefficients in $\mathbb{Q}$ has only finitely many rational points on it's "surface". The vast majority of Diophantine equations would either have no solutions at all or only a finite number of them.

Mordell's conjecture was proved by Gerd Faltings in 1983. He was 28 at the time and won a Fields medal for his work three years later. Mordell's conjecture follows from abc. Of the abc conjecture Faltings has said "If the abc conjecture is true you would know not just that there is a finite number of solutions, you could list them all"

To prove the abc conjecture would be a big step forward for mathematics and an enormous achievement for the person who did it.



In the morning of August 30, 2012, it might very well have happened. Shinichi Mochizuki posted four papers on his web-site, filled with 600 pages of very advanced, abstract and new ideas. It was a new mathematical theory. He called it inter-universal Teichmüller theory and it resulted in a proof of the abc conjecture. This was not the first attempt to conquer the abc conjecture. It is a very hard problem, Lucien Szpiro had made an attempt in 2007 but his proof turned out to be incorrect.

Famous mathematical problems often attract the attention of amateur mathematicians but the abc conjecture is not the type of problem that usually attract their attention and Shinichi Mochizuki is not an amateur mathematician, far from it. He is a mathematician of the highest rank.

Shinichi was born 1969 in Tokyo, Japan but grew up in USA where his family had moved when he was a child; a talented and precocious child that started at Princeton's mathematical department at age 16. It didn't take long before he started on a PhD. People who know him describe him as a very original thinker that works hard and focused on mathematical problems, a private person and a creature of habit with an office and desk in perfect order.

After Faltings had solved Mordell's conjecture he started teaching at Princeton, where he became advisor to Mochizuki for his senior thesis and for his doctoral thesis. Falting was known as a very demanding examiner, some would say intimidating. Even eminent mathematicians would become nervous when Falting criticized a mistake in their work. He was just the right type of mathematician to prepare Mochizuki for his work to come.

Falting's field was algebraic geometry, an area of mathematics that had been transformed by Alexander Grothendieck into a very abstract and theoretical field, even though in the end it dealt with concrete algebraic equations to describe geometric structures. Grothendieck, often described as the greatest mathematician of the 20th century, had a propensity for philosophy whereas Faltings used the highly abstract theories to solve concrete problems, exactly the type of work that Mochizuki would need to solve the abc conjecture.

After his PhD and two years at Harvard Mochizuki moved back to Japan, a country closer to his personality than America. He got a position at RIMS while still only 25 years old. RIMS, acronym for Research Institute of Mathematical Sciences is a part of Kyoto University and a place not unlike IAS (Princeton's Institute for Advanced Study). It's a place where faculty members can focus on research with no teaching required and little external disturbance.

From his position at RIMS Mochizuki made major contributions to fields with names that only initiated know the meaning of; anabelian geometry, Hodge-Arakelov theory, p-adic Teichmüller theory, theory of Frobenoids and étale theta function theory.

Mochizuki's private and withdrawn personality makes him an unlikely candidate for international fame and reputation but this is exactly what

happened in 1996 (at least in some mathematical circles) when he proved a famous conjecture of Grothendieck. As Mochizuki's reputation grew he started to move away from the mainstream of mathematics with work of ever increasing levels of abstraction that was becoming increasingly hard for his peers to understand. In the early 2000's he stopped participating in international meetings and he rarely left Kyoto. He did keep in touch with some fellow number theorists who knew that he was having his eyes set for an attack on the abc conjecture. There was virtually no competition, most other mathematicians considered it a problem too hard to solve.

By early 2012 rumors where emerging that Mochizuki was getting close to a proof and then in August 2012 it happened, without any fuss or any announcements he posted four papers on his website and waited for the world to find out what he had done.

The first reaction of mathematicians in the field when they started to read the papers was often bewilderment. They could simply not understand it. One number theorist describes it as "reading a paper from the future or from outer space". According to Mochizuki's own estimate it would take a graduate student ten years to understand his work and for an expert in a field close to Mochizuki's work it might take 500 hours. Top mathematicians would hesitate to take on such a gigantic task, even Faltings who tried to read his work gave up after a while. The situation is not helped by Mochizuki's reluctance to lecture outside Japan.

Five years after the posting it's still an open question in the mathematical community whether to accept the proof or not. Part of the problem according to Mochizuki is that mathematicians need to "deactivate their thought patterns" and think in new ways to understand his work.

Fesenko, a number theorist from UK and one of the first outside Japan to take on Mochizuki's work claims to have verified the proof. He describes the main theme of the new field 'inter-universal geometry' as looking at integers from a new perspective and seeing multiplication as something malleable and deformable. Classical multiplication would be just one particular case of a family of structures, in the same way as a circle is a special case of an ellipse.

A problem for the acceptance of Mochizuki's proof is that the few who claim to have grasped it have great difficulties to explain it to anyone else.

One mathematician says that the situation reminds him of the Monthy Python joke about a person who writes down the world's funniest joke but anyone who reads it dies from laughing and can never talk about it.

Five years after Mochizuki uploaded Inter-Universal Teichmüller theory (IUT I-IV) with a proof of the abc conjecture, the question whether the conjecture is now a proven theorem or still a conjecture is an open question. As an outsider one wonders, what is the problem?

Several workshops have been organized to remedy the situation but progress has been slow. The result of the first workshop outside Asia, in Oxford December 2015 tells something about the problem. The first days covering pre-IUT material was okay but the last two days devoted to IUT lead mostly to frustrations among the gathered experts with lectures peppered with definitions and terminology in a very high pace with little room for questions. Many left little wiser about the key ideas of IUT than before. Mochizuki does his best to explain his ideas via e-mail and regular additions of remarks and clarifications to his posted papers.

The process of how a proof becomes accepted by the mathematical community at large usually starts with a publication in a mathematical journal where the paper has undergone a thorough peer review prior to publication. Wiles' original proof of FLT contained a critical error that was discovered during peer review. It took Wiles a year of hard work to fix the proof. The IUT papers has been submitted to PRIMS (Publications of RIMS) and rumor has it that publication will come in 2018. For general acceptance something more is probably needed, clarification of central parts and an understanding of the proof among some top mathematicians.

The question of when to accept a mathematical proof is not new in the history of mathematics. In the early 20^{th} century there were different schools of thought constructivism vs. realism that argued about whether to accept the axiom of choice or not. Then there was the question of computer-assisted proof and computer-aided proof-by-exhaustion. These techniques are now generally accepted, especially if complemented with independent programing to avoid programming errors and automated proof checking. These were however questions of a different kind.

To ponder IUT, I give you the abstract of IUT I and IV plus a critical part from paper III where many can't see the reasoning behind the red part.

INTER-UNIVERSAL TEICHMÜLLER THEORY I: CONSTRUCTION OF HODGE THEATERS

Abstract. The present paper is the first in a series of four papers, the goal of which is to establish an arithmetic version of Teichmüller theory for number fields equipped with an elliptic curve − which we refer to as "inter-universal Teichmüller theory" − by applying the theory of semi-graphs of anabelioids, Frobenioids, the ´etale theta function, and log-shells developed in earlier papers by the author. We begin by fixing what we call "initial Θ-data", which consists of an elliptic curve EF over a number field F, and a prime number $l \geq 5$, as well as some other technical data satisfying certain technical properties. This data determines various hyperbolic orbicurves that are related via finite ´etale coverings to the once-punctured elliptic curve XF determined by EF . These finite ´etale coverings admit various symmetry properties arising from the additive and multiplicative structures on the ring $Fl = Z/lZ$ acting on the l-torsion points of the elliptic curve. We then construct "Θ±ellNF-Hodge theaters" associated to the given Θ-data. These Θ±ellNF-Hodge theaters may be thought of as miniature models of conventional scheme theory in which the two underlying combinatorial dimensions of a number field − which may be thought of as corresponding to the additive and multiplicative structures of a ring or, alternatively, to the group of units and value group of a local field associated to the number field − are, in some sense, "dismantled" or "disentangled" from one another. All Θ±ellNF-Hodge theaters are isomorphic to one another, but may also be related to one another by means of a "Θ-link", which relates certain Frobenioid-theoretic portions of one Θ±ellNF-Hodge theater to another in a fashion that is not compatible with the respective conventional ring/scheme theory structures. In particular, it is a highly nontrivial problem to relate the ring structures on either side of the Θ-link to one another. This will be achieved, up to certain "relatively mild indeterminacies", in future papers in the series by applying the absolute anabelian geometry developed in earlier papers by the author. The resulting description of an "alien ring structure" [associated, say, to the domain of the Θ-link] in terms of a given ring structure [associated, say, to the codomain of the Θ-link] will be applied in the final paper of the series to obtain results in diophantine geometry. Finally, we discuss certain technical results concerning profinite conjugates of decomposition and inertia groups in the tempered fundamental group of a p-adic hyperbolic curve that will be of use in the development of the theory of the present series of papers, but are also of independent interest.

Corollary 3.12. **(Log-volume Estimates for Θ-Pilot Objects)** *Suppose that we are in the situation of Theorem 3.11. Write*

$$-|\log(\underline{\underline{\Theta}})| \in \mathbb{R} \bigcup \{+\infty\}$$

for the **procession-normalized mono-analytic log-volume** *[i.e., where the average is taken over $j \in \mathbb{F}_l^*$ — cf. Remark 3.1.1, (ii), (iii), (iv); Proposition 3.9, (i), (ii); Theorem 3.11, (i), (a)] of the* **holomorphic hull** *[cf. Remark 3.9.5] of the* **union** *of the* **possible images** *of a* **Θ-pilot object** *[cf. Definition 3.8, (i)], relative to the relevant* **Kummer isomorphisms** *[cf. Theorem 3.11, (ii)], in the* **multiradial representation** *of Theorem 3.11, (i), which we regard as* **subject** *to the* **indeterminacies** (Ind1), (Ind2), (Ind3) *described in Theorem 3.11, (i), (ii). Write*

$$-|\log(\underline{q})| \in \mathbb{R}$$

for the **procession-normalized mono-analytic log-volume** *of the image of a* **q-pilot object** *[cf. Definition 3.8, (i)], relative to the relevant* **Kummer isomorphisms** *[cf. Theorem 3.11, (ii)], in the* **multiradial representation** *of Theorem 3.11, (i), which we do* **not** *regard as subject to the indeterminacies* (Ind1), (Ind2), (Ind3) *described in Theorem 3.11, (i), (ii). Here, we recall the definition of the symbol "$\triangle$" as the result of identifying the* **labels**

$$\text{"0" and "}(\mathbb{F}_l^*)\text{"}$$

[cf. [IUTchII], Corollary 4.10, (i)]. In particular, $|\log(\underline{q})| > 0$ is easily computed in terms of the various **q-parameters** *of the elliptic curve E_F [cf. [IUTchI], Definition 3.1, (b)] at $\underline{v} \in \underline{\mathbb{V}}^{\mathrm{bad}}$ ($\neq \emptyset$). Then it holds that $-|\log(\underline{\underline{\Theta}})| \in \mathbb{R}$, and*

$$-|\log(\underline{\underline{\Theta}})| \geq -|\log(\underline{q})|$$

— i.e., $C_\Theta \geq -1$ for any real number $C_\Theta \in \mathbb{R}$ such that $-|\log(\underline{\underline{\Theta}})| \leq C_\Theta \cdot |\log(\underline{q})|$.

Proof. Suppose that we are in the situation of Theorem 3.11. We begin by reviewing precisely what is achieved by the various portions of Theorem 3.11 and,

⋮ 8 pages later

the theory of the present series of papers yields **two tautologically equivalent ways to compute** *the log-volume of the q-pilot object at* $(1, 0)$

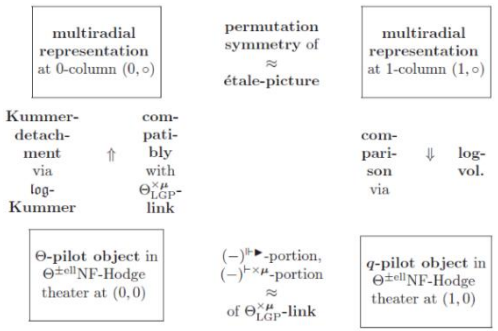


Fig. 3.8: Two tautologically equivalent ways to compute the log-volume of the q-pilot object at $(1, 0)$

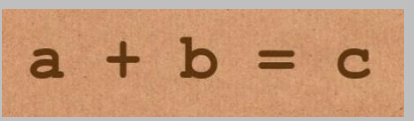
— cf. Fig. 3.8 above. If one interprets the above discussion in terms of the notation introduced in the statement of Corollary 3.12, then one concludes [from the *compactness* of the tensor packets of log-shells in Theorem 3.11, (i), (a)] that the quantity $-|\log(\underline{\underline{\Theta}})|$ is *finite*, and, moreover, that

$$-|\log(q)| \leq -|\log(\underline{\underline{\Theta}})| \in \mathbb{R}$$

⋮

INTER-UNIVERSAL TEICHMÜLLER THEORY IV: LOG-VOLUME COMPUTATIONS AND SET-THEORETIC FOUNDATIONS

Abstract. The present paper forms the fourth and final paper in a series of papers concerning "inter-universal Teichmüller theory". In the first three papers of the series, we introduced and studied the theory surrounding the logtheta-lattice, a highly non-commutative two-dimensional diagram of "miniature models of conventional scheme theory", called Θ±ellNF-Hodge theaters, that were associated, in the first paper of the series, to certain data, called initial Θ-data. This data includes an elliptic curve EF over a number field F, together with a prime number $l \geq 5$. Consideration of various properties of the log-theta-lattice led naturally to the establishment, in the third paper of the series, of multiradial algorithms for constructing "splitting monoids of LGP-monoids". Here, we recall that "multiradial algorithms" are algorithms that make sense from the point of view of an "alien arithmetic holomorphic structure", i.e., the ring/scheme structure of a Θ±ellNF-Hodge theater related to a given Θ±ellNF-Hodge theater by means of a non-ring/scheme-theoretic horizontal arrow of the log-theta-lattice. In the present paper, estimates arising from these multiradial algorithms for splitting monoids of LGP-monoids are applied to verify various diophantine results which imply, for instance, the so-called Vojta Conjecture for hyperbolic curves, the ABC Conjecture, and the Szpiro Conjecture for elliptic curves. Finally, we examine − albeit from an extremely naive/non-expert point of view! − the foundational/set theoretic issues surrounding the vertical and horizontal arrows of the log-theta-lattice by introducing and studying the basic properties of the notion of a "species", which may be thought of as a sort of formalization, via set-theoretic formulas, of the intuitive notion of a "type of mathematical object". These foundational issues are closely related to the central role played in the present series of papers by various results from absolute anabelian geometry, as well as to the idea of gluing together distinct models of conventional scheme theory, i.e., in a fashion that lies outside the framework of conventional scheme theory. Moreover, it is precisely these foundational issues surrounding the vertical and horizontal arrows of the log-theta-lattice that led naturally to the introduction of the term "inter-universal".



4.6 General Case

It remains to prove that the general case of periods of prime powers follows $T_{p^k}(b) = T_p(b) \cdot p^{k-1}$ when none of the special cases of the previous section applies. To do this, three lemmas will be used.

Lemma 1.
If $a_i \equiv 1 \pmod{p}$ for $i = 1, \dots, m$ and $m \in \mathbb{Z}^+$ then
$\sum_{i=1}^{m} a_i \equiv 0 \pmod{p} \Leftrightarrow m \equiv 0 \pmod{p}$ (The proof is left as an exercise)

Lemma 2.
If $b^{mq} \equiv 1 \pmod{p^n}$ for some $n \geq 1$ with q a multiple of the period of p and m is not a multiple of p then $b^q \equiv 1 \pmod{p^n}$.

Proof.
Show $\left.\begin{matrix} b^{mq} \equiv 1 \pmod{p^n} \\ T_p(b) | q \ \wedge m \not\equiv 0 \pmod{p} \end{matrix}\right\} \Rightarrow b^q \equiv 1 \pmod{p^n}$

Let $T = T_p(b)$ so $q = dT$ for some $d \in \mathbb{Z}$.
$b^{mq} - 1 = b^{Tmd} - 1 = (b^{Td} - 1)(b^{Td(m-1)} + b^{Td(m-2)} + \cdots + b^{Td} + 1)$
Lemma 1works on the second factor which has m terms, each of which is congruent to $1 \pmod{p}$, since $b^T \equiv 1 \pmod{p}$.
$p^n | b^{mq} - 1$ and $m \not\equiv 0 \pmod{p}$ gives by using lemma 1, $p^n | b^{Td} - 1$
$\therefore b^q \equiv 1 \pmod{p^n}$ ■

Lemma 2 gives an alternative definition of Wieferich primes in base b:
$b^{p-1} \equiv 1 \pmod{p^2} \Leftrightarrow b^{T_p(b)} \equiv 1 \pmod{p^2}$
$T_p(b) | p - 1$ makes $\Leftarrow$ obvious and $\Rightarrow$ follows from lemma 2.

Lemma 3.
$b^{Tp^{k-1}} \equiv 1 \pmod{p^{k+1}} \Rightarrow b^{Tp^{k-2}} \equiv 1 \pmod{p^k}$ where
p is an odd prime, $k > 1$ and $T = T_p(b)$.

Proof.
$b^T \equiv 1 \pmod{p} \rightarrow b^T = 1 + np$ for some $n \in \mathbb{Z}$.
The binomial theorem gives $\begin{cases} (b^T)^{p^{k-1}} \equiv 1 + np^k \pmod{p^{k+1}} & (1) \\ (b^T)^{p^{k-2}} \equiv 1 + np^{k-1} \pmod{p^k} & (2) \end{cases}$
Assuming $b^{Tp^{k-1}} \equiv 1 \pmod{p^{k+1}}$ and (1) gives $p | n$
From (2) and $p | n$ follows $b^{Tp^{k-2}} \equiv 1 \pmod{p^k}$ ■

Theorem. (Power Rule Theorem)
If $p > 2$ is a prime that is not a factor of the base, not a period one prime and not a Wieferich prime for base b then $T_{p^k}(b) = T_p(b) \cdot p^{k-1}$ for $k > 1$.

Proof.

Set $T_p(b) = T$. Two things need to be shown: I. $p^k | b^{Tp^{k-1}} - 1$
II. $p^k | b^t - 1 \Rightarrow t \geq Tp^{k-1}$

I.
$b^T \equiv 1 \pmod{p} \Rightarrow b^T - 1 = np \ \ (n \in \mathbb{Z}) \Rightarrow b^T = np + 1$
$b^{Tp^{k-1}} - 1 = (np+1)^{p^{k-1}} - 1 = np^k(1 + \cdots) \Rightarrow p^k | b^{Tp^{k-1}} - 1$
II.
Show for $k \geq 2$ that $p^k | b^t - 1 \Rightarrow t \geq Tp^{k-1}$
Assume $t < Tp^{k-1}$ then t must be a multiple of T, the period of p since $p^k | b^t - 1 \Rightarrow p | b^t - 1$. Let $t = mT$.
Case 1.
m is a multiple of p. Write $m = rp^u$ with $1 \leq u < k - 1 \ \ (k - u \geq 2)$ and r not a multiple of $p \rightarrow t = rp^u T$
$p^k | b^{rp^u T} - 1$ By Lemma 2 we can cancel r
$p^k | b^{p^u T} - 1$ By Lemma 3 we can repeatedly cancel $p's$ from both sides
$p^{k-u} | b^T - 1$ If $T = 1$ then p is a period one prime, i.e. a contradiction
$k - u \geq 2 \Rightarrow b^T \equiv 1 \pmod{p^2} \Rightarrow p$ is a Wieferich prime, a contradiction
Case 2.
m is not a multiple of p.
$p^k | b^{mT} - 1$ By Lemma 2 we can cancel m
$p^k | b^T - 1$ and since $k \geq 2$ another contradiction of p a Wieferich prime

$\therefore T_{p^k}(b) = T_p(b) \cdot p^{k-1}$ if p is not covered by the special cases ■

In conclusion, T the period i.e. the length of the smallest repeating section of a base b expansion of a fraction m/n where $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_N^{k_N}$ is zero (no repeating part when n has only prime factors from the base and otherwise:

$$T_n(b) = \operatorname{lcm}\left(T_{p_1{}^{k_1}}(b), T_{p_2{}^{k_2}}(b), \ldots, T_{p_N{}^{k_N}}(b)\right)$$

$p = 2$	$T_{2^k}(b) = \left[k \leq \tilde{N}\right] \cdot 1 + \left[\tilde{N} < k \leq \tilde{N} + \tilde{M}\right] \cdot 2 + \left[k > \tilde{N} + \tilde{M}\right] \cdot 4 \cdot 2^{k-1-\tilde{N}-\tilde{M}}$	
$p \mid b$	$T_{p^k}(b) \equiv 1$	$(b = \alpha 2^{\tilde{N}} + 1 = \beta 2^{\tilde{M}} - 1)$
$p \mid b - 1$	$T_{p^k}(b) = \left[k \leq \tilde{N}\right] \cdot 1 + \left[k > \tilde{N}\right] \cdot p^{k-\tilde{N}}$	$(b - 1 = \alpha p^{\tilde{N}})$
$p^2 \mid b^{p-1} - 1$	$T_{p^k}(b) = \left[k \leq \tilde{N}\right] \cdot T_p(b) + \left[k > \tilde{N}\right] \cdot T_p(b) \cdot p^{k-\tilde{N}}$	($\tilde{N}$ is order of p)
Otherwise:	$T_{p^k}(b) = T_p(b) \cdot p^{k-1}$	

The original problem of finding a digit sequence xyz… and $A + B + C = 1$:

```
A:     0.xyz.......        ( Everything in base 10 )
B:     0.00xyz......       ( B=1% of A=10^-2A )
C:     0.00000xyz...       ( C=1‰ of B=10^-5A )
A+B+C=0.99999999...
```

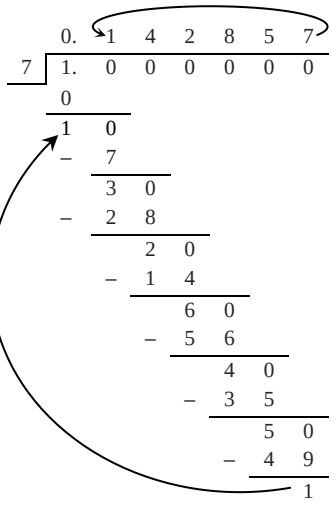
was solved by $A = m/n = 100\,000/101\,001$. To find out for how long we need to do long division before digits start to repeat we can use what we know so far to calculate periods:

$n = 101\,001 = 3^1131^1257^1 \rightarrow T_{101\,001} = \mathrm{lcm}(T_3, T_{131}, T_{257})$
$T_p|\varphi(p) = p - 1 \rightarrow T_3|2 \quad T_{131}|2^15^113^1 \quad T_{257}|2^8$ MultiplicativeOrder→
$T_3 = 1 \quad T_{131} = 2^15^113^1 \quad T_{257} = 2^8 \rightarrow T_{101\,001} = 2^85^113^1 = 16\,640$

The 4-term problem $A + B + C + D = 1$:
$B = 1\%$ of $A \quad C = 1$ppm of $B \quad D = 1‰$ of $C \rightarrow$
$A = m/n$ with $n = 101\,000\,001\,001 = 107 \cdot 943\,925\,243$
$T_{107} = 53$, $T_{943\,925\,243} = 13^1239^1151903^1 \rightarrow T_n = 25\,014\,018\,913$

4.7 Period of Primes

Understanding the period of a general fraction m/n has so far been reduced to understanding the period of prime reciprocals $T_p(b)$ where we can assume that p is not a divisor of the base, $p \nmid b$.



Each step in the long division gives a residue r_k in the multiplicative group $\mathbb{Z}_p^*$ $r_{k+1} \equiv br_k \pmod p$. When a residue repeats the cycle is closed.
N.B. $bs \equiv bt \wedge p \nmid b \Rightarrow s \equiv t \pmod p$
Each possible r_k leads to a unique r_{k+1} and $\mathbb{Z}_p^*$ is finite so $(r_k)_{k=1}^{\infty}$ is periodic.
$b^{p-1} \equiv 1 (\mathrm{mod}\ p) \wedge r_{k+1} \equiv br_k (\mathrm{mod}\ p)$
$\Rightarrow r_{k+p-1} \equiv b^{p-1}r_k \equiv r_k \pmod p \Rightarrow$
The period of p^{-1} must divide $p - 1$.

$$T_p(b)|p-1$$

The period $T_p(b)$ is bounded by $p - 1$.

A prime that attains this maximal period is called a **full reptend prime (**for a given base). In base 10 the full reptend primes, with $T_p(10) = p - 1$ are:

7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, …

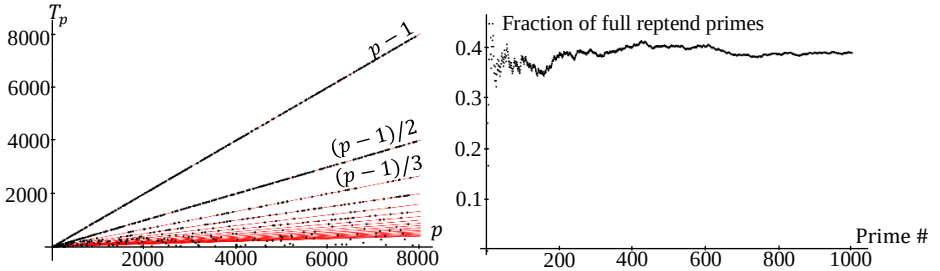


Fig. 4.7 Plot of T_p as a function of p and fraction of full reptend primes in base 10.

The first residue in $(r_k)_{k=1}^{T_p}$ for the fraction m/p with $m \in \{1,..,p-1\}$ and p a full reptend prime is m and then it continues cyclically in the same way, $r_{k+1} \equiv br_k \pmod p$ as for $1/p$. The digits of m/p are given by an injective function from $r_k \in \{1,\dots,p-1\}$ to $d_k \in \{0,\dots,b-1\}$ where $d_k = \lfloor br_k/p \rfloor$.

Example.

$1/7$:	$(r_k)_{k=1}^{T_p} = (1,3,2,6,4,5)$	$(d_k)_{k=1}^{T_p} = (1,4,2,8,5,7)$	$1 \cdot 1/7 = 0.\overline{142857}$
$2/7$:	$(r_k)_{k=1}^{T_p} = (2,6,4,5,1,3)$	$(d_k)_{k=1}^{T_p} = (2,8,5,7,1,4)$	$2 \cdot 1/7 = 0.\overline{285714}$
$3/7$:	$(r_k)_{k=1}^{T_p} = (3,2,6,4,5,1)$	$(d_k)_{k=1}^{T_p} = (4,2,8,5,7,1)$	$3 \cdot 1/7 = 0.\overline{428571}$
		⋮	

The repeating sequence $(d_k)_{k=1}^{T_p}$ of a full reptend prime represents a **cyclic number** which means that cyclic permutations of the $p-1$ digits gives different multiples, from 1 to $p-1$ of the cyclic number.

Example.

$p = 7$	$p = 17$
$(r_k)_{k=1}^{T_p} = (1,3,2,6,4,5)$	$(r_k)_{k=1}^{T_p} = (1,10,15,14,4,6,9,5,16,7,2,3,13,11,8,12)$
$1/7 = 0.\overline{142857}$	$1/17 = 0.\overline{0588235294117647}$
142857·1=142857	0588235294117647·1=0588235294117647
142857·2=285714	0588235294117647·2=1176470588235294
142857·3=428571	0588235294117647·3=1764705882352941
142857·4=571428	0588235294117647·4=2352941176470588
142857·5=714285	0588235294117647·5=2941176470588235
142857·6=857142	0588235294117647·6=3529411764705882
	⋮
	0588235294117647·16=9411764705882352

Notice that $142 + 857 = 999$ and $05882352 + 94117647 = 99999999$. This is no coincidence. Midy's theorem states that if $m/p = 0.\overline{d_1 d_2 \ldots d_{2n}}$ in base b with p a prime then $d_i + d_{i+n} = b$ for $i = 1, \ldots, n$. If T_p is a multiple of 10 then each digit $0,1, \ldots, 9$ will appear the same number of times in the reptend. Such primes are called proper primes (for base 10).

To finally get a grip on the period length of a fraction we need to understand the proportion of primes with a period of $T_p = (p-1)/k$ for each k. Data suggests converging proportions for each value of k. The largest limiting proportion, C is for $k = 1$, the full reptend primes with a limit around 37%. The limiting proportions equal a rational number times C. The number does not seem to depend on the base except for some exceptions. A square base such as 4 or 9 has no full reptend primes.

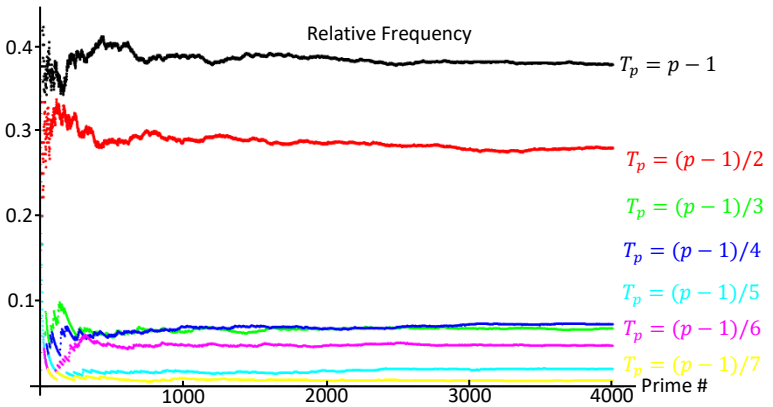


Fig. 4.8 Proportion of primes with $T_p = (p-1)/k$ for $k = 1, \ldots, 7$

Conjecture. (Artin's conjecture)
For a base b that is not a perfect power and not $b = b_0 c^2$ with b_0 square-free and $b_0 \not\equiv 1 \pmod 4$ the proportion of full reptend primes approach a limiting value that equals:

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p(p-1)}\right) \qquad \text{(Product taken over all prime numbers)}$$

The constant is called Artin's constant, $C_{\text{Artin}} = 0.3739558136 \ldots$

The conjecture is true if the generalized Riemann hypothesis holds. This was shown by Hooley in 1967.

Further explorations of Artin's conjecture and the Riemann hypothesis and its generalizations are left for later chapters.