

Theorem 34 A real algebraic number α of degree n is not approximable to order $n + 1$ or higher.

Proof. Theorem 37 is $n = 1$. Let α satisfy the equation $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n = 0$ where $a_i \in \mathbb{Z}$, $n \geq 2$. Since the degree of α is n , this polynomial must be irreducible (since otherwise $f(x) = g(x) \cdot h(x) \Rightarrow 0 = f(\alpha) = g(\alpha) \cdot h(\alpha)$ so $g(\alpha) = 0$ or $h(\alpha) = 0$ and each would have lower degree than n).

If $x \in (\alpha - 1, \alpha + 1)$, $|x| < |\alpha| + 1$ so

$$\begin{aligned} |f'(x)| &= |na_0x^{n-1} + (n-1)a_1x^{n-2} + \dots + a_{n-1}| \\ &\leq |na_0x^{n-1}| + |(n-1)a_1x^{n-2}| + \dots + |a_{n-1}| \\ &< n|a_0|\{|\alpha| + 1\}^{n-1} + (n-1)|a_1|\{|\alpha| + 1\}^{n-2} + \dots + |a_{n-1}| \\ &= A \end{aligned}$$

Now if $\frac{h}{k}$ is a rational approximation to α with $\alpha - 1 < \frac{h}{k} < \alpha + 1$ we must have $f\left(\frac{h}{k}\right) \neq 0$, since otherwise $f(x)$ would have a factor $x - \frac{h}{k}$ over \mathbb{Q} , but it is of degree $n \geq 2$ and irreducible. Hence

$$\left|f\left(\frac{h}{k}\right)\right| = \frac{|a_0h^n + a_1h^{n-1}k + \dots + a_nk^n|}{k^n} \geq \frac{1}{k^n}$$

By the **Mean Value Theorem** $f\left(\frac{h}{k}\right) = f\left(\frac{h}{k}\right) - f(\alpha) = \left(\frac{h}{k} - \alpha\right) f'(\xi)$ for some ξ between $\frac{h}{k}$ and α . Hence

$$\left|\frac{h}{k} - \alpha\right| = \frac{\left|f\left(\frac{h}{k}\right)\right|}{|f'(\xi)|} > \frac{1}{Ak^n}$$

There is no constant C so that $\frac{a}{Ak^n} < \frac{C}{k^{n+1}}$ for infinitely many k , hence α is *not* approximable to order $n + 1$ or higher. \square

Definition A **Liouville Number** $\eta \in \mathbb{R}$ satisfies $\forall m \in \mathbb{N} \exists \frac{h_m}{k_m} \in \mathbb{Q}$ such that $\left|\eta - \frac{h_m}{k_m}\right| < \frac{1}{k_m^m}$.

Proposition Any Liouville Number is transcendental.

Proof. $\forall m \geq n + 1$, $\left|\eta - \frac{h_m}{k_m}\right| < \frac{1}{k_m^m} < \frac{1}{k_m^{n+1}}$. So η cannot be algebraic of order $n + 1 \forall n \in \mathbb{N}$. \square

Ex $\eta_1 = 10^{-1!} + 10^{-2!} + \dots + 10^{-m!} + \dots = 0.1100010\dots$ and $\frac{h_m}{k_m}$ is the m^{th} partial sum so $k_m = 10^{m!}$

$$\begin{aligned} \left|\eta_1 - \frac{h_m}{k_m}\right| &= 10^{-(m+1)!} + 10^{-(m+2)!} + \dots \\ &< 2 \cdot 10^{-(m+1)!} \\ &< (10^{m!})^{-m} \\ &= \frac{1}{k_m^m}. \end{aligned}$$

Ex (Baker)(Alledi, 1979) $|\log(2) - \frac{a}{b}| > \frac{1}{10^{10}b^{5.8}} \forall \frac{a}{b} \in \mathbb{Q}$.

Ex (Baker, 1964) $|\sqrt[3]{2} - \frac{a}{b}| > \frac{C}{b^{296}} \forall \frac{a}{b} \in \mathbb{Q}$.

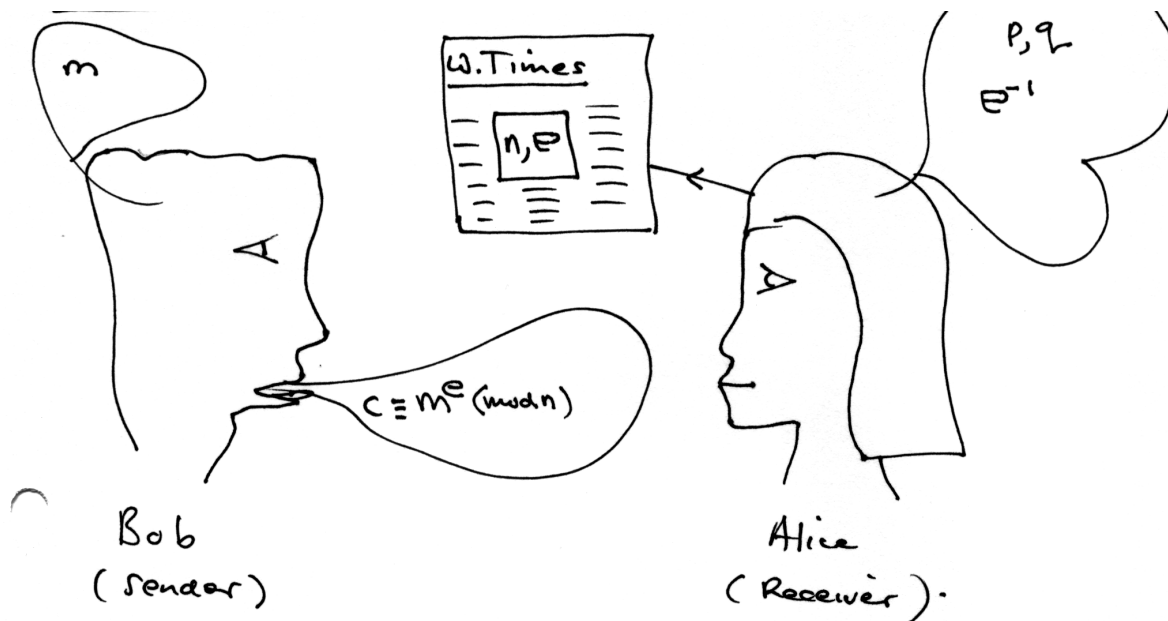
Ex (Mahler, 1953) $|\pi - \frac{a}{b}| > \frac{1}{b^{42}} \forall \frac{a}{b} \in \mathbb{Q}$.

Ex (Gelfond, Schneider, 1934) $\alpha \in \mathbb{A}, \beta \in \mathbb{A} \setminus \mathbb{Q}, \alpha \neq 0 \Rightarrow \alpha^\beta \in \mathbb{T}$. e.g. $2^{\sqrt{2}} \in \mathbb{T}, \sqrt{2}^{\sqrt{2}} \in \mathbb{T}$.

Ex (Hermite, 1873) $e \in \mathbb{T}$.

Ex (Lindeman, 1882) $\pi \in \mathbb{T}$ via $\alpha \in \mathbb{A} \setminus \{0\} \Rightarrow e^\alpha \in \mathbb{I}$ since $e^{i\pi} = -1$.

RSA Public Key Cryptograms



1. Let $p, q \in \mathbb{P}$ be large and distinct primes known only to Alice.
2. Alice selects a (large) random integer r relatively prime to $(p-1)(q-1)$.
3. Alice publishes $n = pq$ and e (say in a newspaper—the **public key**).
4. The sender Bob has a message and encodes this in an integer $1 < m < n$.

5. He uses the public key (n, e) to *compute* the least positive residue $c \equiv m^e \pmod{n}$. The **encrypted message** is c .
6. He sends c to Alice using any (public) transmission process.
7. Alice recovers m from c using

$$\begin{aligned}
 \phi(n) &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \\
 &= pq \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \\
 &= (p-1)(q-1) \\
 &= r
 \end{aligned}$$

as follows:

8. Compute $d \equiv e^{-1} \pmod{r}$ using $xe + yr = 1$ so $de \equiv 1 \pmod{r}$.
9. Then $c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+\ell\phi(n)} \equiv m(m^{\phi(n)})^\ell \equiv m \cdot 1^\ell \pmod{n} \Rightarrow c^d \equiv m \pmod{n}$ and $1 < m < n \Rightarrow$ we have recovered m .

Code Cracking

Given $n = pq$ where $p, q \in \mathbb{P}$ and are *large*, find p and q .

Method 1 Either $p \leq \sqrt{n}$ or $q \leq \sqrt{n}$ so for $1 \leq j \leq \lfloor \sqrt{n} \rfloor$ try $j|n$ until it succeeds.

- If $n \sim 10^{100}$, $\sqrt{n} \sim 10^{50}$.
- If we can check 1 million divisors on average, per second then we need 3.2×10^{37} years = T .
- If we speed this up by 1 million times (i.e. 10^{12} per second), $T = 3.2 \times 10^{31}$ years.

Method 2 (Pollard's $p-1$, 1974) Let n have a prime factor p such that $p-1$ is a product of (high powers) of *small* primes. By Fermat's little theorem, if $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p} \Rightarrow p|(a^{p-1} - 1, n)$. The prime p is unknown. So first let $k = 2^{\alpha_1} 3^{\alpha_2} \dots 4^{\alpha_s}$ where $2, 3, \dots, r$ are the first s primes and $\alpha_i \in \mathbb{N}$ and are "small". Compute $(a^k - 1, n) = ((a^k - 1) \pmod{n}, n)$ and then can be done in $O(\log_2(2kn))$ operations. If $\exists p|n$ with $p-1|k$ and $(a, n) = 1$ then $p|a^k - 1$ since $a^k = a^{(p-1)\ell} = (a^{p-1})^\ell \equiv 1^\ell \equiv 1 \pmod{p}$ and so $(a^k - 1, n) \geq p > 1$.

If $(a^k - 1, n) \neq n$ we have a non-trivial factor of n , so we can divide by it, and repeat this process on each factor.

If $(a^k - 1, n) = n$ choose a new a .

If $(a^k - 1, n) = 1$ choose a larger k .

Ex $n = 246,082,373$

1. Compute $2^{n-1} \neq 1$ (Mathematica: `PowerMod[2, n-1, n]`—very slow). Hence n is *not* prime, by Fermat's little theorem. $\Rightarrow n$ is composite.
2. Let $a = 2$, $k = 2^2 \cdot 3^2 \cdot 5 = 180$ then $k = 180 = 2^2 + 2^4 + 2^5 + 2^7$ in base 2. We need to compute $2^{2^i} \pmod{n}$ for $0 \leq i \leq 7$ we can do a few extras by successive mod n squaring:

i	$2^{2^i} \pmod{n}$
0	2
1	4
2	16
3	256
4	65,536
5	111,566,955
6	166,204,404
7	214,344,997
8	111,354,998
9	82,087,367
10	7,262,569
11	104,815,687

Using the table

$$\begin{aligned}
 2^{180} &= 2^{2^2} \cdot 2^{2^4} \cdot 2^{2^5} \cdot 2^{2^7} \\
 &\equiv 16 \cdot 65,536 \cdot 111,566,955 \cdot 28,795,219 \pmod{246,082,373} \\
 &\equiv 121,299,227 \pmod{n}
 \end{aligned}$$

then, using the Euclidean algorithm:

$$(2^{180} - 1, n) = \gcd(12,129,926, 246,082,373) = 1$$

so the test *fails* because n has no factor p with $p - 1$ dividing 180.

Choose a new $k = \{2, 3, \dots, 9\} = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$. In base 2 $2520 = 2^3 + 2^4 + 2^6 + 2^7 + 2^8 + 2^{11}$ so $2^{2520} \equiv 2^{2^3} \cdot 2^{2^4} \dots 2^{2^{11}} \equiv 101,220,672 \pmod{n}$ and $(2^{2520} - 1, n) = \gcd(101,220,672, 246,082,373) = 2521$ so $2521 | n$ and we have a factor. Indeed $n = 2521 \cdot 97613$ and each of these factors is prime.

Summary (Pollard $p - 1$) $n \geq 2$ composite given.

1. $k = \{1, 2, 3, \dots, K\}$, a product of small primes to small powers.
2. Choose arbitrary a in $1 < a < n$, say $a = 2$.
3. Calculate (a, n) . If more than 1 then a is a factor of n so *return a*.
4. Let $d = (a^k - 1, n)$.
 If $1 < d < n$ *return d*.
 If $d = 1$ go to 1. and choose $K \rightarrow K + 1$.
 If $d = n$ go to 2. and choose another a .

Pollard's algorithm *eventually* returns a proper factor since we will reach $K = \frac{1}{2}(p - 1)$ so $k = 2^{\alpha_1} \dots \frac{1}{2}(p - 1)$ and $(p - 1) | k$.

Note: The algorithm is *fast* only when n has a prime factor P such that $p - 1$ is the product of small primes to small powers, i.e. K is reasonably *small*.

Method 3 (Lenstra, ECM, 1987) Non-zero elements of $(\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p$ form a multiplicative group of order $p - 1$ so $p - 1 | k \Rightarrow a^k = 1$ in the group. This makes Pollard's $p - 1$ work. Here the group \mathbb{F}_p^* (so-called multiplicative group) is replaced by the *group of points on an elliptic curve* $E(\mathbb{F}_p)$ and a by a *point* $P \in E(\mathbb{F}_p)$.

As before, choose k a product of small primes. If $\#E(\mathbb{F}_p) | k \Rightarrow kP = 0$ in $E(\mathbb{F}_p)$ and this will *often* allow us to find a non-trivial factor of n .

Lenstra is good if for some curve $E(\mathbb{Q})$ and some $p \in \mathbb{P}$, $p | n$ and $\#E(\mathbb{F}_p)$ is a product of small primes. If we *lose with Pollard*, the game is over, e.g $n = pq$ and $p - 1, q - 1$ both have *large* prime factors. If we *lose with Lenstra*, we simply choose a *new curve*.

Note: (Subject to a conjecture but crucial underpinning) $\#E(\mathbb{F}_p) = p + 1 - \varepsilon_p$, $|\varepsilon_p| \leq 2\sqrt{p}$ and for fixed p , as we pass over *all* such curves, the numbers ε_p are *well spread* in the interval $[-2\sqrt{p}, 2\sqrt{p}]$ so it is *likely* we will find a curve E with $\#E(\mathbb{F}_p) =$ product of small primes.

Summary (Lenstra, ECM) $n \geq 2$ a composite integer.

1. Check $(n, 6) = 1$ and $n \neq m^r$ for any $r \geq 2$.
2. Choose random integers b, x_1, y_1 with $1 < b, x_1, y_1 < n$.
3. Let $c = y_1^2 - x_1^2 - bx_1 \pmod{n}$
 Let $E : y^2 = x^3 + bx + c$
 Let $P = (x_1, y_1) \in E$
4. Check $g = (rb^3 + 27c^2, n) = 1$. If $g = 1$ we have 'bad reduction' so go back and get a new b . If $1 < g < n$ we have a non-trivial factor, so *return g*.

5. Let $k = \{1, 2, \dots, K\}$ for some $K \in \mathbb{N}$.

6. Compute

$$kP = \left(\frac{a_k}{d_k^2}, \frac{b_k}{d_k^3} \right)$$

7. Calculate $d = (d_k, n)$.

If $1 < d < n$, return \mathbf{d} .

If $d = 1$ go to 2. and choose a new curve.

If $d = n$ go to 5. and decrease k .

So how/why does it work? What is step 6.?

Suppose we eventually found a curve E such that for $p|n$, $\#E(\mathbb{F}_p) | k$, then each $P \in E(\mathbb{F}_p)$ has an order $o(P) | \#E(\mathbb{F}_p) | k$ so $o(P) | k$ hence $kP = 0$ i.e. kP is the point at ∞ , 0 . Then $p|d_k$ (see \boxtimes below). Hence $p|(d_k, n)$ and normally $n \nmid d_k$.

How to compute kP efficiently ($(P + P) + P + \dots$ is too slow. $k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \dots + k_r \cdot 2^r$ in binary $k_i \in \{0, 1\}$).

$$\left. \begin{array}{l} P_0 = P \\ P_1 = 2P_0 = 2P \\ P_2 = 2P_1 = 2^2P \\ \vdots \\ P_r = 2P_{r-1} = 2^rP \end{array} \right\} kP = \sum_{k_i=1} P_i$$

($2 \log_2(k)$ steps).

All computations are done mod n

$Q_1 = (x_1, y_1)$, $Q_2 = (x_2, y_2)$, $x_i, y_i \in \mathbb{Z}_n$ (integers mod n).

$Q_3 = Q_1 + Q_2 = (x_3, y_3)$

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= -\lambda x_3 - (y_1 - \lambda x_1) \end{aligned}$$

where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ where the division is carried out mod n . Note that in $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$, $x_2 - x_1$ may *not* have an inverse. Then

If $(x_2 - x_1, n) = 1 \Rightarrow$ inverse exists.

If $1 < (x_2 - x_1, n) < n$ return this.

If $(x_2 - x_1, n) = n$ go back to 2. or 5. in Lenstra.

To double a point $Q = (x, y) \pmod{n}$ we need

$$\lambda = \frac{f'(x)}{2y} = \frac{3x^2 + 2ax + b}{2y} \pmod{n}$$

and the *same* choices 1.,2. or 3. apply based on $(2y, n)$.

Ex $n = 1,715,761,513$, $2^{n-1} \equiv 93,082,891 \pmod{n} \Rightarrow n \notin \mathbb{P}$.

1. n is not a power: $\sqrt{n}, \sqrt[3]{n}, \dots, \sqrt[31]{n} = 1.9855$ are not integers (Mathematica: check $n == \text{Floor}[n^{(1/j)}]^j$, for $j = 1, \dots, 31$. $(n, 6) = 1$.)
2. $\sqrt{n} \approx 42,422$ so $\exists p \mid n$, $p < 42,422$. We want k so that some integer close to p divides k . Try $k\{1, 2, \dots, 17\} = 12,252,240$ with lots of factors less than 42,422.

Choosing an elliptic curve: Choose a point P and one coefficient for E , then the other so the point is *on the curve*.

Ex $P = (2, 1)$, $c = -7 - 2b$ e.g. $b = 1 \Rightarrow c = -9$ so $E : y^2 = x^3 + x - 9$ and $(2, 1) \in E$.

Now compute **kP** using successive doubling

$$\begin{aligned} k &= 12,252,240 \\ &= 2^4 + 2^6 + 2^{10} + 2^{12} + 2^{13} + 2^{14} + 2^{15} + 2^{17} + 2^{19} + 2^{20} + 2^{21} + 2^{23} \end{aligned}$$

so we need $2^i P \pmod{n}$ for $0 \leq i \leq 23$.

So

$$\begin{aligned} kP &\equiv (1, 225, 303, 014, 142, 796, 033) \\ &\equiv (421, 401044, 664, 333, 727) \end{aligned}$$

This tells us *nothing* about the factors of n . It is when the addition law *breaks* that we get a factor. So we need a new k , a new P or a new curve.

$k = 12,252,240$ as before, $P = (2, 1)$ as before. $b = 2 \Rightarrow c = -7 - 2b = -11$ so $E : Y^2 = x^3 + 2x - 11$ and $P \in E$ and $kP \pmod{n}$ is *still okay*. $b = 42 \Rightarrow c = -91$ so $E : y^2 = x^3 + 42x - 91$, $P \in E$. The *addition law breaks* and a factor is delivered. Table (A) $2^i P \pmod{n}$ is okay. then we start adding up the points to produce (B).

At the penultimate step

$$\begin{aligned} (2^4 + 2^6 + \dots + 2^{21})P &= 3,863,632P \\ &\equiv (1, 115, 004, 543, 1, 676, 196, 055) \pmod{n} \end{aligned}$$

(B)

(A)

100



$$\begin{aligned}
 2^4 P &= 16P = (385062894, 618628731) \\
 (2^4 + 2^6)P &= 80P = (831572269, 1524749605) \\
 (2^4 + 2^6 + 2^{10})P &= 1104P = (1372980126, 736595454) \\
 (2^4 + 2^6 + 2^{10} + 2^{12})P &= 5200P = (1247661424, 958124008) \\
 (\text{previous partial sum}) + 2^{13}P &= 13392P = (1548582473, 1559853215) \\
 (\text{previous partial sum}) + 2^{14}P &= 29776P = (201510394, 7154559) \\
 (\text{previous partial sum}) + 2^{15}P &= 62544P = (629067322, 264081696) \\
 (\text{previous partial sum}) + 2^{17}P &= 193616P = (844665131, 537510825) \\
 (\text{previous partial sum}) + 2^{19}P &= 717904P = (886345533, 342856598) \\
 (\text{previous partial sum}) + 2^{20}P &= 1766480P = (370579416, 1254954111) \\
 (\text{previous partial sum}) + 2^{21}P &= 3863632P = (77302130, 514483068) \\
 (\text{previous partial sum}) + 2^{23}P &= 12252240P = (1225303014, 142796033)
 \end{aligned}$$

i	$2^i P \pmod{1715761513}$
0	(2, 1)
1	(1286821173, 1072350709)
2	(1334478523, 112522703)
3	(912789305, 77695868)
4	(385062894, 618628731)
5	(866358838, 450284374)
6	(904716938, 169383608)
7	(808696477, 1201030016)
8	(572301268, 107111567)
9	(1512647092, 1695275444)
10	(1858186, 1224662922)
11	(1550404618, 825515387)
12	(1519325194, 1657497846)
13	(522917322, 524407354)
14	(25207285, 1375034461)
15	(781360494, 1457273929)
16	(1108412304, 25813532)
17	(435914774, 323718902)
18	(1399483199, 1203611423)
19	(778823593, 192206539)
20	(853199887, 1012680972)
21	(501929966, 910060788)
22	(1315182921, 305331854)
23	(257200250, 318342966)

Then from the new (A) $2^{23}P \equiv (1, 267, 572, 925, 848, 156, 341) \pmod{n}$ and try to add these points. We need the inverse mod N of the difference of their x -coordinates, but $\gcd(1, 115, 004, 543 - 1, 267, 572, 925, n) = 26, 927 \neq 1$. which gives us the factor $n = 26, 927 \cdot 63, 719$.

Note: ☒ Now we see what this means. 0 is not a finite point on the curve, so $kP = 0$ means we are not able to compute mod p coordinates for kP . The only way that can happen is if $p \mid x_2 - x_1$ a denominator, i.e. $kP = 0$ means at some stage the process of building kP (using the appropriate versions of table (A) and (B) above breaks down.

Mathematica: << NumberTheory'FactorIntegerECM' may be bad. $a^b \pmod{n}$ is PowerMod[a, b, n] and appears bad.

Method 4 Search for solutions to $x^2 \equiv y^2 \pmod{N}$ since then $x^2 - y^2 = (x - y)(x + y) = kN$ and we might get a factor of N .

11 ABC Conjecture

A simple but powerful relation between the additive and multiplicative properties of numbers.

Definition The radical

$$N(n) = \prod_{p|n} p$$

is the largest square-free divisor of n , or the **core** of n .

Ex $n = 2^2 3^5 5^3 \Rightarrow N(n) = 2 \cdot 3 \cdot 5$
 $N(p^\alpha) = p \forall p \in \mathbb{P}$

Proposition N is multiplicative and $N(n) \cdot N(m) = N(nm) \cdot N((n, m))$.

ABC Conjecture: $\forall \varepsilon > 0 \exists K_\varepsilon > 0$ such that if a, b, c are **relatively prime** integers and $a + b = c$ then

$$\max(|a|, |b|, |c|) \leq K_\varepsilon N(abc)^{1+\varepsilon}$$

This is an important unsolved problem. It is so deep it implies the asymptotic Fermat's Last Theorem.

Ex $a = 3^k, b = 2 \cdot 3^k, c = 3^{k+1}$ so $a + b = c$ and $\max(|a|, |b|, |c|) = c = 3^{k+1}$.
 $abc = 2 \cdot 3^{3k+1}$ so $N(abc) = 2 \cdot 3$ and $3^{k+1} \leq K_\varepsilon (2 \cdot 3)^{1+\varepsilon} \forall k$ and some K_ε is false for some $\varepsilon > 0$. i.e. $(a, b, c) = 1$ is essential.

Theorem (Asymptotic Fermat Theorem) $ABC \Rightarrow \exists n_0 \in \mathbb{N}$ so that the Fermat equation $x^n + y^n = z^n$ has no solution in relatively prime integers $\forall n \geq n_0$.

Proof. Let x, y, z be relatively prime (i.e. each has different prime factors). Note that $N(x^n y^n z^n) = N(xyz) \leq xyz \leq z^3$ since $x < z, y < z$. Apply ABC with $\varepsilon = 1$ so $z^n = \max(x^n, y^n, z^n) \leq K_1 N(x^n y^n z^n)^2 \leq K_1 z^6$ so $n \log(z) \leq \log(K_1) + 6 \log(z)$

$$\Rightarrow n \leq 6 + \frac{\log(K_1)}{\log(z)} \leq 6 + \frac{\log(K_1)}{\log(3)}$$

so let

$$n_0 = 7 + \frac{\log(K_1)}{\log(3)}.$$

□

Conjecture (Catalan Conjecture) 8 and 9 are the only consecutive powers i.e. the only solution to Catalan's equation

$$x^m - y^n = 1 \quad \boxtimes$$

in positive integers $x, y, n, m > 1$ is $3^2 - 2^3 = 1$.

Many special cases of this conjecture have been proved: e.g.

1. $x^2 - y^n = 1$ has *one* solution $x = n = 3, y = 2$.
2. $x^m - y^2 = 1$ has no solutions.

So we need only consider $n, m \geq 3$.

Theorem (Asymptotic Catalan Conjecture) $ABC \Rightarrow$ the Catalan equation has only a finite number of solutions.

Proof. Let (x, y, m, n) be a solution with $m, n \geq 3$. Then $(x, y) = 1$ since otherwise $p \mid x, p \mid y \Rightarrow \parallel 1$. The ABC Conjecture with $\varepsilon = \frac{1}{4} \Rightarrow \exists K_{1/4} = K$ such that $\max(|a|, |b|, |c|) \leq KN(abc)^{5/4}$ But $\boxtimes \Rightarrow x^m = 1 + y^n$ so

$$\begin{aligned} y^n < x^m &\leq KN(1 \cdot x^m \cdot y^n)^{5/4} \\ &= KN(xy)^{5/4} \\ &\leq K(xy)^{5/4} \end{aligned}$$

$$\begin{aligned} \Rightarrow m \log(x) &\leq \log(K) + \frac{5}{4}(\log(x) + \log(y)) \\ \Rightarrow n \log(y) &< \log(K) + \frac{5}{4}(\log(x) + \log(y)) \\ \Rightarrow m \log(x) + n \log(y) &< 2 \log(K) + \frac{5}{2}(\log(x) + \log(y)) \\ \Rightarrow \left(m - \frac{5}{2}\right) \log(x) + \left(n - \frac{5}{2}\right) \log(y) &< 2 \log(K) \end{aligned}$$

But $2 \leq x, 2 \leq y$ so

$$\begin{aligned} \left(m - \frac{5}{2}\right) \log(2) + \left(n - \frac{5}{2}\right) \log(2) &< \left(m - \frac{5}{2}\right) \log(x) + \left(n - \frac{5}{2}\right) \log(y) \\ &< 2 \log(K) \end{aligned}$$

$$\Rightarrow m + n < \frac{2 \log(K)}{\log(2)} + 5$$

Thus there are only finitely many exponents m and n for which \boxtimes has a solution. It is *known* thus, for fixed m, n , \boxtimes has only a finite set of solutions x, y . Hence \boxtimes has only a finite set of solutions x, y, m, n . \square

Wieferich Primes

If $p \in \mathbb{P}$ is odd $2^{p-1} \equiv 1 \pmod{p}$

If p is such that $2^{p-1} \equiv 1 \pmod{p^2}$, p is called a **Wieferich prime** and we write $P \in W \subset \mathbb{P}$.

Ex $9 \nmid 2^2 - 1$ so 3 is not one.

$25 \nmid 2^4 - 1$ so 5 is not one.

$49 \nmid 2^6 - 1$ so 7 is not one

Problem: Are there an infinite number of Wieferich (or non-Wieferich) primes?

Lemma Let $p \in \mathbb{P}$ be odd. If $\exists n \in \mathbb{N}$ so $2^n \equiv 1 \pmod{p}$ but $2^n \not\equiv 1 \pmod{p^2}$ then $p \notin W$.

Proof. Let $2^d \equiv 1 \pmod{p}$ with d minimal ($d \nmid 0$). Then $d \mid n$ (else $n = ed + r, 0 < r < d$ and $1 \equiv 2^n = 2^{ed} \cdot 2^r = (2^d)^e \cdot 2^r \equiv 2^r \pmod{p}$ contradiction d being minimal).

Now $2^n \not\equiv 1 \pmod{p^2} \Rightarrow 2^d \not\equiv 1 \pmod{p^2}$ (else $(2^d)^3 \equiv 1^e \Rightarrow 2^n \equiv 1 \pmod{p^2}$). Now $2^d \equiv 1 \pmod{p} \Rightarrow 2^d = 1 + kp$ and $(k, p) = 1$ (else $2^d = 1 + k'p^2$ and $2^d \equiv 1 \pmod{p^2}$). Also $2^{p-1} \equiv 1 \pmod{p} \Rightarrow d \mid p-1 \Rightarrow p-1 = de$ for some e with $1 \leq e \leq p-1$. Then $(ek, p) = 1$ and $w^{p-1} = (2^d)^e = (1 + kp)^e \equiv 1 + ekp \not\equiv 1 \pmod{p^2}$ so $p \notin W$. \square

Definition A **powerful number** is a $v \in \mathbb{N}$ such that $p \mid v \Rightarrow p^2 \mid v$.

Ex $72 = 2 \cdot 6^2 = 2^3 \cdot 3^2$ is powerful but $192 = 2 \cdot 96 = 2^2 \cdot 48 = 2^2 \cdot 4^2 \cdot 3 = 2^6 \cdot 3$ is not.

Theorem $ABC \Rightarrow |W^c| = \infty$.

Proof. $\forall n \in \mathbb{N}$ let $2^n - 1 = u_n v_n \otimes$ where v_n is the maximal *powerful* divisor of $2^n - 1$ so u_n is just those primes which appear to power 1, is square free.

If $p \mid u_n$ then $2^n \equiv 1 \pmod{p}$ by \otimes but $2^n \not\equiv 1 \pmod{p^2}$ since 1 is the power of p appearing in $2^n - 1$. Hence $p \in W^c$, so all the prime divisors of $u_n \in W^c$. If $|W^c| < \infty$, \exists only *finitely* many square-free integers with prime divisors all in $W \Rightarrow \#\{u_n : n = 1, 2, \dots\} < \infty \Rightarrow \#\{v_n : n = 1, 2, \dots\} = \infty$ and so is *unbounded in size*.

Since v_n is powerful $n(v_n) \leq \sqrt{v_n}$. Let $0 < \varepsilon < 1$ in ABC and consider $(2^n - 1) + 1 = a + b = c = 2^n$.

$$\begin{aligned} v_n &\leq u_n \cdot v_n = 2^n - 1 \\ &< 2^n = \max(|a|, |b|, |c|) \\ &\leq K_\varepsilon N(2^n(2^n - 1) \cdot 1)^{1+\varepsilon} \\ &= K_\varepsilon N(2u_n v_n)^{1+\varepsilon} \\ &\leq K_\varepsilon (2u_n)^{1+\varepsilon} N(v_n)^{1+\varepsilon} \\ &\leq K'_\varepsilon v_n^{(1+\varepsilon)/2} \end{aligned}$$

so $v_n < K'_\varepsilon v_n^{(1+\varepsilon)/2} \Rightarrow v_n^{1-\frac{1}{2}-\frac{\varepsilon}{2}} < K'_\varepsilon \Rightarrow v_n < (K'_\varepsilon)^{\frac{1}{1/2-\varepsilon/2}} = B_\varepsilon$ contradicting the *unbounded* nature of the $\{v_n\}$. \square

Theorem (LeVeque, 1952) *If $a, b \geq 2$ are given, the equation $a^x - b^y = 1$ has at most one solution in positive integers x, y unless $a = 3, b = 2$ where there are two solutions: $(x, y) = (1, 1)$ and $(x, y) = (2, 3)$.*

Proof. Assume that (u, v) and (x, y) are solutions with $u < x$. So $a^u - b^v = a^x - b^y = 1$. Then $v < y$ since $0 < a^x - a^u = b^y - b^v$ and $a^u(a^{x-u} - 1) = b^v(b^{y-v} - 1)$. Now $a^u - b^v = 1 \Rightarrow (a, b) = 1 \Rightarrow b^v = a^u - 1 = a^{x-u} - 1$ and $a^u = b^v + 1 = b^{y-v} - 1$.

Hence $a^u = a^{x-u}$ so $u = x - u \Rightarrow 2u = x$ and also $b^{y-v} - b^v = 2$ so $y - v < v$ and $b^v(b^{y-2v} - 1) = 2$. Hence $v = 1, b = 2, b^{y-2v} - 1 = 1$ so $y - 2v = 1 \Rightarrow y = 1 + 2v = 3$. Thus $a^u = 1 + b^v = 3$ so $u = 1$ and $a = 3$. \square

12 Formulas for Primes

A function is easy: Let

$$f(n) := \max\{p \in \mathbb{P} : p | n\}$$

indeed

$$f(n) = \lim_{r \rightarrow 0} \lim_{s \rightarrow 0} \lim_{t \rightarrow 0} \sum_{u=0}^s \left(1 - \cos^2 \left[\frac{(u!)^n \pi}{n} \right] \right)^{2t}$$

Both are impractical.

A formula for p_n the n^{th} prime, would be nice, but probably impossible to find, the elements of \mathbb{P} being scattered in such an irregular manner.

Easier aim: find a formula which produces *only primes*. Will show *no polynomial* will work

$$f(n) = \lfloor \theta^{3^n} \rfloor \text{ does work for some } \theta \in \mathbb{R}.$$

Ex $f(n) = an + b$. Let $f(n) = p$ and $f(m) = q$, $p, q \in \mathbb{P}$, $p \neq q$. Then $(a, b) = 1$ since $d = (a, b) \Rightarrow d | a$ and $d | b$ so $d | an + b = p$. Similarly, $d | q$, but $p \neq q$ so $(p, q) = 1 \Rightarrow d = 1$. So if f has more than one prime value, $(a, b) = 1$.

Tables of primes reveal **arithmetic progressions** of various lengths:

1. 3, 5, 7.
2. 7, 37, 67, 97, 127, 157;
3. 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089.

Proposition *No arithmetic progression of \mathbb{N} , of infinite length, can yield only primes.*

Proof. Let $an + b = p \in \mathbb{P}$ and $n_k = n + kp$, $k = 0, 1, 2, \dots$. Then the n_k^{th} term of the progression is

$$an_k + b = a(n + kp) + b = an + b + akp = p(1 + ak)$$

so $p | an_k + b \forall k \geq 1$. Thus, since the n_k numbers come at intervals every p terms, every p^{th} term of the original progression is divisible by p . Hence the progression contains infinitely many composite numbers. \square

Note: Dirichlet's Theorem (see back) says $\{an + b : n \in \mathbb{N}\}$ contains an infinite number of primes if $(a, b) = 1$.

Proposition *If $p \nmid a$ then every p^{th} term of $\{an + b\}$ is divisible by p .*

Proof. $p \nmid a \Rightarrow (p, a) = 1 \Rightarrow \exists r, s$ so $pr + as = 1$. Let $n_k = kp - bs$, $k = 1, 2, 3, \dots$. Then

$$\begin{aligned} an_k + b &= a(kp - bs) + b \\ &= akp - abs + b \\ &= akp - b(1 - pr) + b \\ &= p(ak + br). \end{aligned}$$

Thus $p \mid an_k + b$. Since $n_{k+1} - n_k = p$ the terms $an_k + b$ occur p terms apart. \square

Ex $2 \nmid a \Rightarrow$ every second term is divisible by 2. So $\{an + b\}$ cannot have more than 3 consecutive prime values, and the middle one must be 2.

Ex $\{30, 030n - 6887 : n = 1, 2, 3, \dots\}$ has 12 consecutive terms which are prime. $30, 030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. This is a curiosity: Linear formulas *fail*.

Quadratic Formulas

$$f(n) = an^2 + bn + c$$

Ex $f(n) = n^2 + 21n + 1$ is *not* composite for $n = -38, -37, \dots, 0, 1, 2, \dots, 17$: 56 values. $f(0) = 1 \notin \mathbb{P}$ of course. However, $f(18) = 703 = 37 \cdot 19$.

Ex $19 \mid f(n)$ if $n \equiv -1 \pmod{19}$: since $n = -1 + 19\ell \Rightarrow$

$$\begin{aligned} f(n) &= (-1 + 19\ell)^2 + 21(-1 + 19\ell) + 1 \\ &= 1 - 21 + 1 + 19\ell \\ &= 19(-1 + \ell) \end{aligned}$$

Ex $f(n) = n^2 + n + 41 \in \mathbb{P}$ for $n \in \{-40, -39, \dots, 39\}$ i.e. for 80 consecutive values.

Conjecture 80 is the best possible for any quadratic.

Known (1967): No $f(n) = n^2 + n + A$ ($A > 41$) gives primes for $n = 0, 1, \dots, A - 2$.

Proposition No quadratic can always be prime.

Proof. $f(n) = an^2 + bn + c = p \in \mathbb{P} \Rightarrow f(n_k) \equiv an^2 + bn + c \pmod{p}$, $n_k = n + kp$ so every p^{th} term of $\{f(n)\}$ is divisible by p . \square

Does $\{an^2 + bn + c\}$ contain an infinite number of prime values?—Unknown.

Does $\{n^2 + 1\}$ have an infinite number of prime values?—Also unknown.

If $f \in \mathbb{Z}[x]$ is a polynomial and $f(n) = p \in \mathbb{P}$, then $p \mid f(n + kp)$ for $k = 0, 1, 2, \dots$, so no such f has an infinite set of consecutive prime values.

Ex Give $d \in \mathbb{N}$, \exists a polynomial $f \in \mathbb{Z}[x]$ of degree d , taking on $d + 1$ *arbitrarily* assigned values, which could be prime:

$$60f(x) = 7x^5 - 85^4 + 355x^3 - 575x^2 + 418x + 180$$

has

$$\begin{array}{rcccccc} n & = & 0 & 1 & 2 & 3 & 4 & 5 \\ f(n) & = & 3 & 5 & 7 & 11 & 13 & 17 \end{array}$$

Method: Use Lagrange interpolation with $x_i = \{0, 1, \dots, 5\}$ and $y_i = \{3, 5, 6, \dots, 17\}$ and

$$f(x) = \sum_{i=1}^6 \left(\prod_{j=1, j \neq i}^6 \frac{(x - x_j)}{(x_i - x_j)} \right) y_i$$

so $f(x_i) = y_i$, $1 \leq i \leq 6$.

By these examples, we see the functions must be more complex than linear or polynomial, if they are to have *all prime values*.

Theorem *There is a number $\theta \in \mathbb{R}$ such that*

$$f(n) = \lfloor \theta^{3^n} \rfloor$$

is prime for all $n \in \mathbb{N}$.

Note: This formula is not *effective*, since to know θ exactly, we would need to be able to recognise arbitrarily large primes ($\theta \approx 1.3064\dots$).

Lemma *If $u_1 \leq u_2 \leq \dots \leq u_n \leq \dots \leq B$ is a bounded increasing real sequence, then*

$$\lim_{n \rightarrow \infty} u_n = \theta$$

exists.

Lemma *If $A \leq \dots \leq v_n \leq \dots \leq v_2 \leq v_1$ is a decreasing real sequence which is bounded below, then*

$$\lim_{n \rightarrow \infty} v_n = \alpha$$

also exists.

Assumption: $\exists A \in \mathbb{N}$ such that if $u > A$, $\exists p \in \mathbb{P}$ with $n^3 < p < (n + 1)^3 - 1$.

“The proof of this assumption is very difficult” (*Elementary Number Theory* by Underwood Dudley). Indeed, but *easier* than $\exists p$ so $n^2 < p < (n + 1)^2$, I would say.

Proof of the Theorem Let p_1 be any prime with $A < p_1$ and for $n = 1, 2, 3, \dots$ let p_{n+1} be a prime with

$$p_n^3 < p_{n+1} < (p_n + 1)^3 - 1$$

Let $u_n = p_n^{3^{-n}} = p_n^{\frac{1}{3^n}}$ and $v_n = (p_n + 1)^{3^{-n}}$, $n = 1, 2, \dots$. Then $u_n + 1 = p_{n+1}^{3^{-n-1}} > (p_n^3)^{3^{-n-1}} = p_n^{3^{-n}} = u_n$. So $\{u_n\}$ is *increasing*. Also $\{v_n\}$ is *decreasing* since $v_{n+1} = (p_{n+1} + 1)^{3^{-n-1}} < ((p_n + 1)^3 - 1 + 1)^{3^{-n-1}} = (p_n + 1)^{3^{-n}} = v_n$.

From their definitions above, $u_n < v_n \forall n \in \mathbb{N}$. Hence, by the two Lemmas above

$$\lim_{n \rightarrow \infty} u_n = \theta \text{ and } \lim_{n \rightarrow \infty} v_n = \alpha$$

Since $u_n < v_n$ we have $\theta \leq \alpha$, indeed $u_n < \theta \leq \alpha < v_n$ because $\{u_n\}$ is strictly increasing and $\{v_n\}$ strictly decreasing.

Therefore $u_n^{3^n} < \theta^{3^n} \leq \alpha^{3^n} < v_n^{3^n} \forall n \in \mathbb{N}$. But, from their definitions, $u_n^{3^n} = p_n$ and $v_n^{3^n} = p_n + 1$ so $p_n < \theta^{3^n} < p_n + 1 \Rightarrow p_n = \lfloor \theta^{3^n} \rfloor \forall n \in \mathbb{N}$ so $\lfloor \theta^{3^n} \rfloor$ is prime. \square

This Theorem would be valuable if we could work out the value of θ without reference to primes.

Ex

$$f(n) = \sin \left(\frac{\pi(1 + (n-1)!)}{n} \right)$$

then $f(n) = 0 \Leftrightarrow n \in \mathbb{P}$.

Another Catalan Conjecture (1876) Let $p_0 = 2 \in \mathbb{P}$ and $p_{n+1} = 2^{p_n} - 1$ for $n = 0, 1, 2, \dots$ then

$$\begin{aligned} p_1 &= 2^2 - 1 = 3 \in \mathbb{P} \\ p_2 &= 2^3 - 1 = 7 \in \mathbb{P} \\ p_3 &= 2^7 - 1 = 127 \in \mathbb{P} \end{aligned}$$

and $p_4 \in \mathbb{P}$. Is $p_j \in \mathbb{P} \forall j$? $\{p_j\}$ increases very rapidly.

Theorem (Matijasevič, 1971) *There exists a multinomial p ($p \in \mathbb{Z}[a, b, c, \dots, z]$) of degree 25 (Jones, Sato, Wada, 1975)) such that the set of prime numbers coincides with the set of positive values assumed by this multinomial, as the variables range in the set of non-negative integers $\mathbb{Z}^+ = \mathbb{N} \cup \{0\}$.*

Proposition (Dixon) *If p is the multinomial, $r = 2 + \frac{1}{2}(p - 2 + |p - 2|)$ is a function (not a multinomial) with range exactly the set of primes.*

Proof. $p(\underline{x}) \leq 0 \Rightarrow p - 2 < 0 \Rightarrow |p - 2| = 2 - p$ so $r = 2 + \frac{1}{2} \cdot 0 = 2 \in \mathbb{P}$ and $p(\underline{x}) > 0 \Rightarrow p(\underline{x}) \geq 2 \Rightarrow r = 2 + \frac{1}{2}(p - 2 + p + 2) = 2 + p - 2 = p$ so $r(\underline{x}) = p(\underline{x}) \in \mathbb{P}$. \square

(Jones, 1979) $F_0 = 1$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$, $n \geq 1$, the **Fibonacci numbers**

are the set of positive values at non-negative integers of

$$p(x, y) = 2xy^4 + x^2y^3 - 2x^3y^2 - y^5 - x^4y + 2y$$

Hilbert's 10th Problem: There is *no* algorithm which is good enough to decide whether any given diophantine equation has a solution in positive integers. (Matijasevič).

(Siegel, 1972) Every quadratic diophantine equation is decidable.

Unknown: Is every multinomial in 2 variables decidable?

These results and questions relate to the **axiomatic and logical** foundation of arithmetic. e.g. are some problems simply impossible to solve because we *do not have* an appropriate set of properties of numbers to begin with?

Resistant problems:

1. *Twin* primes conjecture: \exists an infinite set of $p_n \in \mathbb{P}$ so that $p_n + 2 \in \mathbb{P}$ also.
2. There exist infinitely many *Sophie Germain* primes i.e. $p_n \in \mathbb{P}$ and $2p_n + 1 \in \mathbb{P}$.
3. $M_p = 2^p - 1$ is a *Mersenne* number. Are infinitely many composite? We believe so.

A simple new “axiom”/“conjecture” will resolve each of these questions.

13 Axiom D

(Dirichlet) $(a, b) = 1$, $a \neq 0$, $b \geq 1$, $f(x) = bx + a$ then \exists an infinite number of integers $m \geq 0$ with $f(m) \in \mathbb{P}$.

Conjecture/Axiom (Dixon, 1904) Let $s \geq 1$ and $f_j(x) = b_jx + a_j$ with $b_j \geq 1$ and $a_j, b_j \in \mathbb{Z}$. If $\nexists n > 1$ with

$$n \mid f_1(k)f_2(k) \cdots f_s(k) \quad \forall k \in \mathbb{Z}$$

OR

$$\forall n > 1, \exists k \in \mathbb{Z} \text{ so } n \nmid f_1(k)f_2(k) \cdots f_s(k) \quad \boxtimes$$

Then there exist infinitely many $m \in \mathbb{N}$ with $\{f_1(m), \dots, f_s(m)\}$ all primes.

This is **Axiom D**, the weakest form of a more general **Axiom H** where the linear polynomials f_j are replaced with polynomials of arbitrary degree.

Proposition Axiom D $\Leftrightarrow \boxtimes \Rightarrow \exists m \in \mathbb{N}$ so $\{f_1(m), \dots, f_s(m)\}$ are primes.

Proof. (\Rightarrow) Follows directly.

(\Leftarrow) $\exists m_1 \geq 1$ so $f_1(m_1), \dots, f_s(m_s)$ are primes. Let $g_j(x) = f_j(x + 1 + m_1)$ for $1 \leq j \leq s$. Then \boxtimes is satisfied by the $\{g_j\}$, hence $\exists k_1 \geq 1$ so $g_1(k_1), \dots, g_s(k_1)$ are primes. Let $m_2 = k_1 + 1 + m_1 > m_1 + 1$ so $f_1(m_2), \dots, f_s(m_2)$ are primes. Repetition of this procedure generates infinitely many $m_j \in \mathbb{N}$. \square

Theorem Axiom D $\Rightarrow \forall m \geq 1$ there exist infinitely many arithmetic progressions consisting of m Sophie Germain primes.

Proof. Let $d = (2m + 2)! \geq 4!$ (even). Consider the $2m$ polynomials:

$$\begin{aligned} f_1(x) &= x + d \\ f_2(x) &= x + 2d \\ &\vdots \\ f_m(x) &= x + md \\ f_{m+1}(x) &= 2x + 2d + 1 \\ f_{m+2}(x) &= 2x + rd + 1 \\ &\vdots \\ f_{2m}(x) &= 2x + 2md + 1 \end{aligned}$$

so $f_{m+j}(x) = 2f_j(x) + 1$, $1 \leq j \leq m$. These polynomials satisfy \boxtimes : Let $f(x) = \prod_{j=1}^{2m} f_j(x)$ with degree $2m$ and leading coefficient 2^m . Let $p \in \mathbb{P}$ divide $f(k)$ for $k = -1, 0, 1, \dots, p - 2$ (1). Now $f(-1) = \prod_{j=1}^{2m} (\text{odd}) \equiv 1 \pmod{2} \Rightarrow p \neq 2$ so $f(x) \equiv 0 \pmod{p}$ has $2m$ roots (in a field extension \mathbb{F}_p), but it has p roots from (1). Hence $p \leq 2m$ and $p \mid d = (2m + 2)!$ But $f(-1) \equiv 1 \pmod{3}$.

$f(-1) = (d-1)(2d-1)\cdots(2d-1)(4d-1) \equiv (-1)^{2m}(3) \equiv 1 \pmod{3}$. Hence $p \neq 3$. But

$$\begin{aligned} f(1) &= \underbrace{(1+d)(1+2d)\cdots(3+2d)(3+4d)\cdots}_{m \text{ factors}} \\ &\equiv 3^m \pmod{p} \end{aligned}$$

since $p \mid d$. Hence $p \nmid f(1)$ which is a contradiction. Hence the $\{f_j\}$ satisfy \boxtimes . By **Axiom D** there exist infinitely many k so $f_j(k) = p_i$ and $f_{m+i}(k) = 2p_i + 1$ are primes for $i = 1, \dots, m$. Moreover $p_1 < p_2 < \cdots < p_m$ are in progression with difference d . \square

Corollary *Axiom D* \Rightarrow there exist infinitely many Sophie Germain primes.

Proposition Let a, b, c be pairwise relatively prime non-zero integers (i.e. each consists of products of different primes). Thus there exist infinitely many pairs of primes (p, q) so $ap - bq = c$ assuming Axiom D.

Proposition (Schinzel and Sierpiński, 1958) *Axiom D* \Rightarrow there exist infinitely many n with $\frac{1}{2}\phi(n) \in \mathbb{P}$ where ϕ is Euler's phi function.

Proposition There exist infinitely many triples of consecutive integers, each being the product of two distinct primes, assuming Axiom D.

Proof.

$$\left. \begin{aligned} f_1(x) &= 10x + 1 \\ f_2(x) &= 15x + 2 \\ f_3(x) &= 6x + 1 \end{aligned} \right\} \begin{aligned} f_1(0)f_2(0)f_3(0) &= 2 \\ f_1(1)f_2(1)f_3(1) &= 11 \cdot 17 \cdot 7 \end{aligned}$$

$\Rightarrow \boxtimes$ is satisfied. Thus there exist infinitely many integers $m \geq 1$ such that:

$$\left. \begin{aligned} p &= 10m + 1 \\ q &= 15m + 2 \\ r &= 6m + 1 \end{aligned} \right\} \text{are primes.}$$

Then

$$\begin{aligned} 3p &= 30m + 3 = 3p \\ 3p + 1 &= 30m + 4 = 2q \\ 3p + 2 &= 30m + 5 = 5r \end{aligned}$$

so $\{3p, 3p + 1, 3p + 2\}$ are products of two distinct primes. \square

Theorem *Axiom D* \Rightarrow there exist infinitely many composite Mersenne numbers ($M_p = 2^p - 1$).

Proof. Let

$$\left. \begin{aligned} f_1(x) &= 4x - 1 \\ f_2(x) &= 8x - 1 \end{aligned} \right\} f_1(0)f_2(0) = 1 \Rightarrow \boxtimes$$

Hence there exist infinitely many $m \geq 1$ such that

$$\left. \begin{aligned} p &= 4m - 1 \\ q &= 8m - 1 \end{aligned} \right\} \text{are primes}$$

But then $q = 2p + 1$ and $p \equiv 3 \pmod{4}$.

Claim $q \mid 2^p - 1$: Consider the Legendre symbol $(2 \mid q) = (-1)^{\frac{q^2-1}{8}}$. $p \equiv 3 \pmod{4} \Rightarrow q = 2(3 + 4m) + 1 \Rightarrow q = 7 + 8m \equiv -1 \pmod{8} \Rightarrow q^2 \equiv 1 \pmod{8}$. So $(2 \mid q) = (-1)^{\frac{1-1}{8}} = 1 \equiv 2^{\frac{q-1}{2}} = 2^p \pmod{q}$. Hence $q \mid 2^p - 1$.

Now, if $m > 1$ the corresponding primes p, q satisfy $s^p - 1 = 2^{4m-1} > 8m - 1 = 1 \Leftrightarrow 16^m - 2 > 16m - 2 \Leftrightarrow 16^m > 16m$ which is true. So $q \mid 2^p - 1$ is a *proper* divisor and $M_p = 2^p - 1$ is composite. \square

Theorem Let $a_1 < a_2 < \dots < a_s$ be non-zero integers and assume $f_1(x) = x + a_1, \dots, x + a_s = f_s(x)$ satisfy \boxtimes . Then there exist infinitely many integers $M \geq 1$ so $\{m + a_1, m + a_2, \dots, m + a_s\}$ are consecutive primes.

Theorem Axiom D $\Rightarrow \forall k \in \mathbb{N}$ there exist infinitely many pairs of consecutive primes with difference $2k$. In particular, there exist infinitely many pairs of twin primes.

Proof. Let

$$\left. \begin{array}{l} f_1(x) = x + 1 \\ f_2(x) = x + 2k + 1 \end{array} \right\} \text{ then } \begin{array}{l} f_1(0)f_2(0) = 1 + 2k = a \\ f_2(1)f_2(1) = 2(2 + 2k) = b \end{array}$$

and

$$\begin{aligned} (a, b) &= (1 + 2k, 4(1 + k)) \\ &= (1 + 2k, 1 + k) \\ &= 1 \end{aligned}$$

since $2(1 + k) - (1 + 2k) = 1$. Hence $\{f_1, f_2\}$ satisfy \boxtimes .

By the previous Theorem, since $1 < 2k + 1$, there exist infinitely many integers $m \geq 1$ so $f_1(m), f_2(m)$ are consecutive primes, i.e. $p = m + 1$ and $q = m + 2k + 1 = p + 2k$ are consecutive primes, so $\{p, p + 2k\}$ are twins with the given property. \square

Axiom D has a number of other consequences e.g. on the existence of primes in *arithmetic progressions*.

Let $1 < n$ and d a multiple of $\prod_{p \leq n} p$. Then there exist infinitely many arithmetic progressions with difference d , each consisting of \mathbf{n} consecutive primes.

Proving Axiom D: First try $s = 2$, generalising $s = 1$. Showing Axiom D is *independent*—very difficult and unlikely.

14 Partitions

Generating functions arise because if $n, m \in \mathbb{Z}$

$$\begin{array}{ccc} \text{addition} & \underbrace{n+m} & \longleftrightarrow & \underbrace{z^n \cdot z_m} & \text{multiplication} \\ & \text{integers} & & \text{polynomials/series} & \end{array}$$

Ex (Lagrange) $\forall n \exists x_i, 1 \leq i \leq 4, n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is equivalent to if $(1 + z + z^4 + \dots + z^{n^2} + \dots)^4 = f(z) = a_0 + a_1z + a_2z^2 + \dots$ then $a_i > 0 \forall i = 0, 1, 2, \dots$

Change Making How many ways can we make change for $n \in \mathbb{N}$ if the coins are of denomination 1, 2 and 3 i.e. given N how many *different* solutions are there to

$$n = 1x + 2y + 3z$$

in $x, y, z \geq 0$ all integers?

Let $|z| < 1$ and write, using the sum to ∞ of a geometric series:

$$\begin{aligned} \frac{1}{1-z} &= 1 + z + z^2 + z^3 + \dots \\ &= 1 + z^1 + z^{1+1} + z^{1+1+1} + \dots \\ \frac{1}{1-z^2} &= 1 + z^2 + z^{2+2} + z^{2+2+2} + \dots \\ \frac{1}{1-z^3} &= 1 + z^3 + z^{3+3} + z^{3+3+3} + \dots \end{aligned}$$

so

$$\begin{aligned} \frac{1}{(1-z)(1-z^2)(1-z^3)} &= (1 + z^1 + z^{1+1} + \dots)(1 + z^2 + z^{2+2} + \dots)(1 + z^3 + z^{3+3} + \dots) \\ &= \sum_{n=0}^{\infty} c(n)z^n \end{aligned}$$

$$c(0) = 1.$$

what happens when we multiply out the RHS? We get terms like $z^{1+1+1+1} \cdot z^2 \cdot z^{3+3} = z^{12}$ but this is $z^{\text{four '1's} + \text{one '2' + two '3's}}$ i.e. a method of changing 12 into '1's, '2's and '3's. Every way of changing 12 will appear so $c(12)$ is exactly the number of ways 12 can be 'changed'. Similarly, $c(n)$ is the number of ways n can be changed

$$\sum_{n=0}^{\infty} c(n)z^n = \frac{1}{(1-z)(1-z^2)(1-z^3)}$$

so our number theory *counting* problem has been transformed into an *analytic* problem, i.e. finding coefficients of a Taylor series. *Don't do the series multiplication* to get the

' $c(n)$'s. Use partial fractions (check by simplifying the RHS):

$$\frac{1}{(1-z)(1-z^2)(1-z^3)} = \frac{1}{6} \frac{1}{(1-z)^3} + \frac{1}{4} \frac{1}{(1-z)^2} + \frac{1}{4} \frac{1}{(1-z^2)} + \frac{1}{3} \frac{1}{(1-z^3)}$$

Then

$$\frac{d}{dz} \left(\frac{1}{1-z} \right) = \frac{1}{(1-z)^2} = \frac{d}{dz} \left(\sum_{n=1}^{\infty} z^n \right) = \sum_{n=1}^{\infty} (n+1)z^n$$

and

$$\frac{d}{dz} \left(\frac{1}{2(1-z)^2} \right) = \frac{1}{(1-z)^2} = \frac{d}{dz} \left(\sum_{n=0}^{\infty} \frac{n+1}{2} z^n \right) = \sum_{n=0}^{\infty} \frac{(n+1)(n+2)}{2} z^n$$

$$\begin{aligned} \Rightarrow c(n) &= \frac{1}{6} \cdot \frac{(n+1)(n+2)}{2} + \frac{1}{4}(n+1) + \begin{cases} \frac{1}{4} & n \text{ even} \\ \frac{1}{3} & 3|n \end{cases} \\ &= \left\lfloor \frac{n^2}{12} + \frac{n}{2} + 1 \right\rfloor \quad (\text{see below}) \end{aligned}$$

If $2|n$ and $3|n$ get

$$\begin{aligned} c(n) &= \frac{n^2}{12} + \left(\frac{3}{12} + \frac{1}{4} \right) n + \frac{2}{12} + \frac{1}{4} + \frac{1}{4} + \frac{1}{3} \\ &= \frac{n^2}{12} + \frac{n}{2} + 1 \end{aligned}$$

But $c(n) \in \mathbb{N}$ so

$$c(n) = \left\lfloor \frac{n^2}{12} + \frac{n}{2} + 1 \right\rfloor$$

If $2|n$ and $3 \nmid n$

$$\begin{aligned} c(n) &= \frac{n^2}{12} + \frac{n}{2} + 1 - \frac{1}{3} \\ &= \left\lfloor \frac{n^2}{12} + \frac{n}{2} + 1 \right\rfloor \end{aligned}$$

since $c(n) \in \mathbb{N}$. Similarly, if $2 \nmid n$ and $3|n$:

$$\begin{aligned} c(n) &= \frac{n^2}{12} + \frac{n}{2} + 1 - \frac{1}{4} \\ &= \left\lfloor \frac{n^2}{12} + \frac{n}{2} + 1 \right\rfloor \end{aligned}$$

Crazy Dice

Normal die have faces labelled 1–6. When tossed there exist $6 \times 6 = 36$ *equally likely* outcomes e.g. the *probability* of (6, 6) is $\frac{1}{36}$. What are the probabilities for sums? $s = x + y$, $2 \leq s \leq 12$.

$$p(z) = z^1 + z^2 + z^3 + z^4 + z^5 + z^6$$

Combined possibilities for sums are encoded in

$$\begin{aligned} & (z + z^2 + z^3 + z^4 + z^5 + z^6)(z + z^2 + z^3 + z^4 + z^6) \\ &= z^2 + 2z^3 + 3z^4 + 4z^5 + 5z^6 + 6z^7 + 5z^8 + 4z^9 + 3z^{10} + 2z^{11} + z^{12} \end{aligned}$$

so there are 3 ways in which we can achieve $s = 10$:

$5 + 5$	$=$	10
$6 + 4$	$=$	10
$4 + 6$	$=$	10

Question: Can we label the two cubes with *other* positive integers and obtain the same frequencies for sums? i.e do there exist $a_1, \dots, a_6; b_1, \dots, b_6 \in \mathbb{N}$ so

$$\begin{aligned} p_a(z) \cdot p_b(z) &= (z^{a_1} + z^{a_2} + z^{a_3} + z^{a_4} + z^{a_5} + z^{a_6})(z^{b_1} + z^{b_2} + z^{b_3} + z^{b_4} + z^{b_5} + z^{b_6}) \\ &= z^2 + 2z^3 + 3z^4 + 4z^5 + 5z^6 + 6z^7 + 5z^8 + 4z^9 + 3z^{10} + 2z^{11} + z^{12} \end{aligned}$$

Call these *Crazy Dice*:

$$\begin{aligned} \text{LHS} &= (z + z^2 + z^3 + z^4 + z^5 + z^6)^2 \\ &= \left[z \frac{(1 - z^6)}{1 - z} \right]^2 \\ &= \left[z \frac{(1 - z^2)(1 + z^2 + z^4)}{1 - z} \right]^2 \\ &= [z(1 + z)(1 + z + z^2)(1 - z + z^2)]^2 \end{aligned}$$

Since $\mathbb{Z}[x]$ is a **unique factorisation** domain, the polynomials p_a and p_b must consist of these factors. Since $a_i \geq 1$, $b_i \geq 1$, $1 \leq i \leq 6$, a factor z must occur in *both*. $p_a(1) = 1^{a_1} + 1^{a_2} + 1^{a_3} + 1^{a_4} + 1^{a_5} + 1^{a_6} = 1 + 1 + 1 + 1 + 1 + 1 = 6$ so $(1 + z + z^2)(1 + z)$ must appear in a factorization of p_a . The same applies to p_b . This leaves the two factors $(1 - z + z^2)$ to distribute. One to each \rightarrow normal die. Both to $p_a \rightarrow$ crazy die.

$$\begin{aligned} p_a(z) &= z(1 + z + z^2)(1 - z + z^2)^2 \\ &= z + z^3 + z^4 + z^5 + z^6 + z^8 \\ p_b(z) &= z(1 + z + z^2)(1 + z) \\ &= z + 2z^2 + 2z^3 + z^4 \end{aligned}$$

so $\{1, 3, 4, 5, 6, 8\}$ and $\{1, 2, 2, 3, 3, 4\}$ are the labels.

Representation Function

Let $\mathcal{A} \subset \mathbb{Z}^+ = \mathbb{N} \cup \{0\}$ a subset of non-negative integers.

How many ways can a given $n \in \mathbb{N}$ be written as the *sum of two elements of \mathcal{A}* ?

- *Order counts* and the summands can be *equal*:

$$r(n) = \#\{(a, b) \in \mathcal{A} \times \mathcal{A} : n = a + b\}$$

- *Order does not count*, but they *can be equal*:

$$r_+(n) = \#\{(a, b) \in \mathcal{A} \times \mathcal{A} : a \leq b, n = a + b\}$$

- *Order does not count, and they cannot be equal:*

$$r_-(n) = \#\{(a, b) \in \mathcal{A} \times \mathcal{A} : a < b, n = a + b\}$$

Let $A(z)$ be the **generating function** for the set \mathcal{A} i.e.

$$A(z) = \sum_{n \in \mathcal{A}} z^n$$

Then

$$\sum_{n=0}^{\infty} r(n)z^n = (A(z))^2 = A^2(z)$$

and

$$\sum_{n=0}^{\infty} r_-(n)z^n = \frac{1}{2} [A^2(z) - A(z^2)] = B(z) \text{ say}$$

finally

$$\sum_{n=0}^{\infty} r_+(n)z^n = B(z) + A(z^2) = \frac{1}{2} [A^2 + A(z^2)]$$

Question: Is there a set $\mathcal{A} \subset \mathbb{Z}^+$, with $\mathcal{A} \neq \emptyset$, for which $r_+ = C = \text{constant } \forall n$ or $\forall n \geq n_0$?

Then $\frac{1}{2} (A^2(z) + A(z^2)) = \frac{C}{1-z} + P(z)$ where P is a *polynomial* with $\partial P < n_0$.

Let $z \rightarrow -1^+$. Then $|P(z)| \leq B_1$ a bound,

$$\left| \frac{C}{1-z} \right| \leq B_2 \text{ a bound,}$$

$A^2(z) \geq 0$ and $A(z^2) \rightarrow A(1) \rightarrow \infty$ so the RHS is *unbounded*. Hence the answer to the question is no.

Question: Can we split \mathbb{Z}^+ into two disjoint sets \mathcal{A} and \mathcal{B} so every non-negative integer is expressible in the *same* number of ways as the sum of two *distinct* members of \mathcal{A} as it is the sum of two distinct members of \mathcal{B} ?

Trial-and-error: Let $\mathbf{0} \in \mathcal{A}$, then $\mathbf{1} \in \mathcal{B}$ else $1 = 1 + 0 = a + a'$ but *not* $1 = b + b'$. Then $\mathbf{2} \in \mathcal{B}$ else $2 = 2 + 0 = a + a' \neq b + b'$ ($1 + 1$ is not distinct. then $\mathbf{3} \in \mathcal{A}$ else $3 \neq a + a'$ whereas $3 = 1 + 2 = b + b'$ etc. Then

$$\begin{aligned} \mathcal{A} &= \{0, 3, 5, 6, 9, \dots\} \\ \mathcal{B} &= \{1, 2, 4, 7, 8, \dots\} \end{aligned}$$

What is the *pattern*? Are \mathcal{A} and \mathcal{B} *unique*?

Use generating functions $A(z)$ for \mathcal{A} and $B(z)$ for \mathcal{B} so

$$\frac{1}{2} [A^2(z) - A(z^2)] = \frac{1}{2} [B^2(z) - B(z^2)] \quad (1)$$

Also, because $\mathcal{A} \sqcup \mathcal{B} = \mathbb{Z}^+$ is a splitting

$$A(z) + B(z) = \frac{1}{1-z} = 1 + z + z^2 + z^3 + \dots \quad (2)$$

$$(1) \Rightarrow A^2(z) - B^2(z) = A(z^2) - B(z^2) \text{ so } (A(z) - B(z))(A(z) + B(z)) = A(z^2) - B(z^2).$$

$$\begin{aligned} (2) \Rightarrow \frac{A(z) - B(z)}{1-z} &= A(z^2) - B(z^2) \\ \Rightarrow A(z) - B(z) &= (1-z^2)[A(z^2) - B(z^2)] \quad \forall z, |z| < 1 \\ z \rightarrow z^2 \Rightarrow A(z^2) - B(z^2) &= (1-z^2)[A(z^4) - B(z^4)] \\ \Rightarrow A(z) - B(z) &= (1-z)(1-z^2)[A(z^4) - B(z^4)] \end{aligned}$$

Iterating this gives:

$$A(z) - B(z) = (1-z)(1-z^2)(1-z^4) \dots (1-z^{2^{n-1}}) [A(z^{2^n}) - B(z^{2^n})]$$

But $A(0) = 1$, $B(0) = 0$ and $z^{2^n} \rightarrow 0$ as $n \rightarrow \infty$ since $|z| < 1$

\Rightarrow

$$\begin{aligned} A(z) - B(z) &= \prod_{j=0}^{\infty} (1 - z^{2^j}) [A(0) - B(0)] \\ &= \prod_{j=0}^{\infty} (1 - z^{2^j}) \quad (3) \end{aligned}$$

We can easily multiply this out!

Every $n \in \mathbb{Z}^+$ has a unique binary representation, i.e. expression as a sum of powers of 2, 2^j . Indeed,

- $n = \text{sum of an even number of powers of } 2 \Rightarrow z^n \text{ has coefficient } +1.$
- $n = \text{sum of an odd number of powers of } 2 \Rightarrow z^n \text{ has coefficient } -1.$

so $\mathcal{A} = \{n : n \text{ is an even } \dots\}$, $\mathcal{B} = \{n : n \text{ is an odd } \dots\}$

This is *not* trivial, not something we might have guessed.

$$\mathcal{A} = \begin{cases} 0 = 0 \\ 3 = 2^0 + 2^1 \\ 5 = 2^0 + 2^2 \\ 6 = 2^1 + 2^2 \\ 9 = 2^0 + 2^3 \\ \vdots \end{cases} \quad \mathcal{B} = \begin{cases} 1 = 2^0 \\ 2 = 2^1 \\ 4 = 2^2 \\ 7 = 2^0 + 2^1 + 2^2 \\ 8 = 2^3 \\ \vdots \end{cases}$$

Euler's Identity

Consider the number of ways of expressing n as the sum of (any number of) *distinct* positive integers $p(n)$:

$$\begin{aligned} 6 &= 1 + 2 + 3 \\ &= 2 + 4 \\ &= 1 + 5 \\ &= 6 \end{aligned}$$

so $p(6) = 4$. Also express n as the sum of positive *odd* numbers, $q(n)$ allowing *repeats* so:

$$\begin{aligned} 6 &= 1 + 5 \\ &= 3 + 3 \\ &= 1 + 1 + 1 + 3 \\ &= 1 + 1 + 1 + 1 + 1 + 1 \end{aligned}$$

so $q(6) = 4$ and $p(6) = q(6)$. This is not a coincidence!

Theorem (Euler) *The number of ways of expressing N as the sum of distinct positive integers equals the number of ways of expressing n as (not necessarily distinct) odd positive integers.*

Proof. To prove $\sum_{n=0}^{\infty} p(n)z^n = \sum_{n=0}^{\infty} q(n)z^n$ i.e

$$(1+z)(1+z^2)(1+z^3)\cdots = \frac{1}{(1-z)(1-z^3)(1-z^5)\cdots}$$

This is **Euler's identity**.

Consider $\frac{1}{\text{RHS}} \times \text{LHS} = (1-z)(1-z^3)(1-z^5)\cdots(1+z)(1+z^2)(1+z^3)\cdots$. This is

$$\begin{aligned} &(1-z)(1+z)(1-z^3)(1+z^3)\cdots(z+z^2)(1+z^4)(1+z^6)\cdots \\ &= (1-z^2)(1-z^6)(1-z^{10})\cdots(a+z^2)(1+z^4)(1+z^6)\cdots = P(z), \text{ say} \end{aligned}$$

But then

$$\begin{aligned} P(z^2) &= (1-z^4)(1-z^8)\cdots(1+z^4)(1+z^8)\cdots \\ &= (1-z^2)(1+z^2)(1-z^6)(1+z^6)\cdots(1+z^4)(1+z^8)\cdots \\ &= (1-z^2)(1-z^6)\cdots(1+z^2)(1+z^4)\cdots \\ &= P(z) \end{aligned}$$

So $P(z) = P(z^2)$ so $P'(z) = 2zP'(z^2)$ and $P'(0) = 0$ similarly $P''(0) = 0$, $P'''(0) = 0$, \dots , $p^{(n)}(0) = 0 \forall n \in \mathbb{N}$ so (Taylor expansion) $P(z) = P(0) + 0 = P(0) \forall |z| < 1$. But $P(0) = (1-0)(1-0)\cdots(1+0)(1+0)\cdots = 1$. Hence $P(z) = 1 \forall |z| < 1$ so LHS = RHS and we have *proved* Euler's mysterious identity. \square

Ex Euler's identity at $z = \frac{1}{2}$ is

$$\prod_{j=1}^{\infty} \left(1 + \frac{1}{2^j}\right) = \prod_{i=1}^{\infty} \left(1 - \frac{1}{2^{2^{i-1}}}\right)^{-1}$$

i.e. $\frac{3}{2} \cdot \frac{5}{4} \cdot \frac{9}{8} \cdots = \frac{2}{1} \cdot \frac{8}{7} \cdot \frac{32}{31} \cdots$ or take log and use $\log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \frac{z^4}{4} \cdots$ ($|z| < 1$).

$$\sum_{j=1}^{\infty} \sum_{n=1}^{\infty} (-1)^n \frac{z^{jn}}{n} = \sum_{i=1}^{\infty} \sum_{n=1}^{\infty} \frac{z^{(2^{i-1})n}}{n}$$

Partition Function $p(n)$

Question: In *how many ways* can $n \in \mathbb{N}$ be expressed as a sum of natural numbers?

First *let order count*:

Ex

$$\left. \begin{aligned} 4 &= 1 + 3 = 3 + 1 \\ &= 2 + 2 \\ &= 4 \\ &= 2 + 1 + 1 = 1 + 2 + 1 = 1 + 1 + 2 \\ &= 1 + 1 + 1 + 1 \end{aligned} \right\} 8 = 2^{4-1} \text{ ways}$$

Proposition *If order counts, n can be expressed as a sum in $2^{n-1} = q(n)$ ways.*

Proof. $n = 1$: $q(1) = 1 = 2^{1-1}$ so the result is true.

Given $N > 1$ assume it is true for $n - 1$ and write

$$n = (n - 1) + 1 = (n - 2) + 2 = \cdots = 1 + (n - 1)$$

by the induction hypothesis each of these sums can be expressed in

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

ways and this represents the sums for n with 2 or more terms with order counting. The only remaining sum is $n = n$ so we get $q(n) = 2^{n-1} \forall n \in \mathbb{N}$. \square

If order does *not* count then the counting is much more complex: $p(1) = 1$, $p(2) = 2$, $p(3) = 3$,

$$\begin{aligned} 4 &= 1 + 1 + 1 + 1 \\ &= 1 + 1 + 2 \\ &= 1 + 3 \\ &= 2 + 2 \\ &= 4 \end{aligned}$$

and $p(4) = 5$. Similarly $p(5) = 7$. *There is no pattern.*

Major MacMahon computed hundreds of values of $p(n)$ by hand and it suddenly occurred to him that from a distance, the outline of the digits formed a *parabola*!

$$\begin{aligned}
 p(1) &= 1 \\
 p(5) &= 7 \\
 p(10) &= 42 \\
 p(15) &= 176 \\
 p(20) &= 627 \\
 p(25) &= 1,958 \\
 p(30) &= 5,604 \\
 p(40) &= 37,338 \\
 p(50) &= 204,226 \\
 p(100) &= 190,569,292 \\
 p(200) &= 3,972,999,029,388
 \end{aligned}$$

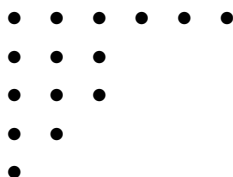
\Rightarrow # of digits $\sim C\sqrt{n}$ so $p(n) \sim e^{\alpha\sqrt{n}}$. Later work showed

$$p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4\sqrt{3} \cdot n} \text{ (Rademacher)}$$

At $n = 200$, RHS $\approx 4 \times 10^{12} \approx p(200)$. the proof uses elliptic modular functions. We will derive an upper bound for the RHS. $p(n)$ is called the **(unrestricted) partition function**.

Geometric Representation

Ex $15 = 6 + 3 + 3 + 2 + 1$



Reading vertically, $15 = 5 + 4 + 3 + 1 + 1 + 1$ is another, “conjugate” partition. Then number of parts in the first equals the size of the largest part in the second, and vice-versa.

Proposition *The number of partitions of n into m parts is equal to the number of partitions of n into parts, the largest of which is m .*

Theorem (Euler)

$$\prod_{m=1}^{\infty} \frac{1}{1-x^m} = \sum_{n=0}^{\infty} p(n)x^n$$

$|x| < 1, p(0) = 1$. So the LHS is a generating function for $p(n)$.

Proof. Expand each factor on LHS as a power series using the sum to ∞ of a geometric series:

$$\text{LHS} = (1 + x + x^2 + x^3 + \dots)(1 + x^2 + x^4 + \dots)(1 + x^3 + x^6 + \dots) \dots$$

Now multiply out and collect like powers of x so

$$\text{LHS} = 1 + \sum_{j=1}^{\infty} a(j)x^j$$

We need to prove $a(j) = p(j)$. If we take a term x^{k_1} from the first, x^{2k_2} from the second, x^{3k_3} from the third, ..., x^{mk_m} from the m^{th} where each $k_i \geq 0$, their product is

$$x^{k_1} \cdot x^{2k_2} \dots x^{mk_m} = x^k$$

say, where $k = k_1 + 2k_2 + 3k_3 + \dots + mk_m$ or

$$k = \underbrace{(1 + 1 + \dots + 1)}_{k_1} + \underbrace{(2 + 2 + \dots)}_{k_2} + \underbrace{(3 + 3 + \dots)}_{k_3} + \dots + \underbrace{(m + m + \dots)}_{k_m}$$

so this is a partition of K into positive summands. Conversely each term x^k comes from such a partition. Hence $a(k) = p(k)$. (This can be made into a more rigorous proof.) \square

Similarly other types of partitions can be described using generating functions:

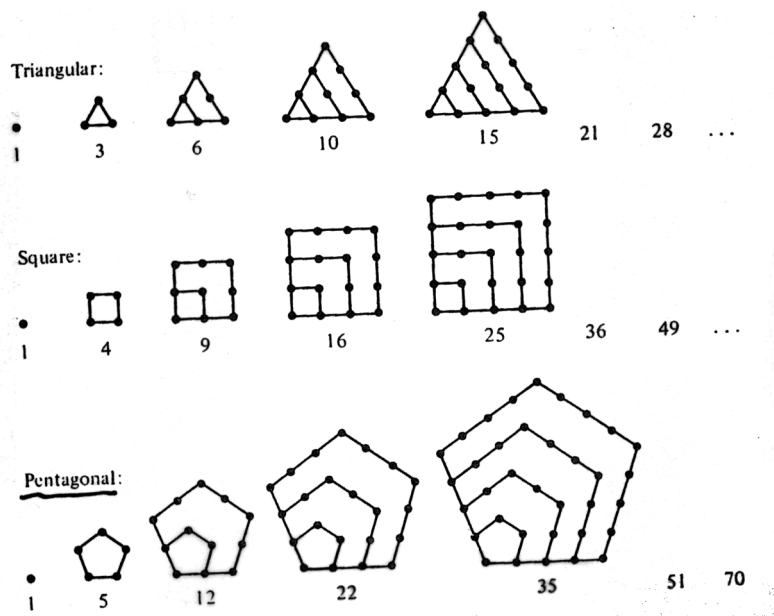
Generating function for the number of partitions of n into parts which are

$\prod_{m=1}^{\infty} \frac{1}{1-x^{2m}}$	even
$\prod_p \frac{1}{1-x^p}$	prime
$\prod_{m=1}^{\infty} (1 + x^m)$	unequal
$\prod_{m=1}^{\infty} (1 + x^{m^2})$	distinct squares
$\prod_p (1 + x^p)$	distinct primes

Pentagonal Numbers

These belong to the family of **polygonal numbers**, beloved by the Greek Pythagoreans.

$$\begin{aligned} 1 + 4 &= 5 \\ 1 + 4 + 7 &= 12 \\ 1 + 4 + 7 + 10 &= 22 \end{aligned}$$



In general, the n^{th} pentagonal number is the n^{th} partial sum of the arithmetic progression $1, 4, 7, 10, 13, \dots, 3n + 1, \dots$ $n = 0, 1, 2, \dots$. Let

$$\begin{aligned} \omega(n) &= \sum_{j=0}^{n-1} (3j + 1) \\ &= 3 \sum_{j=0}^{n-1} j + \sum_{j=0}^{n-1} 1 \\ &= \frac{3}{2}n(n-1) + n \\ &= \frac{3n^2 - n}{2} \end{aligned}$$

Then, normally, $\omega(n) = \frac{3n^2 - n}{2}$ and $\omega(-n) = \frac{3n^2 + n}{2}$ are called **pentagonal numbers**. $\omega(1) = 1$, $\omega(2) = 5$, $\omega(3) = 12, \dots$

Theorem (Euler's Pentagonal Number Theorem) *Let $|x| < 1$, then*

$$\prod_{m=1}^{\infty} (1 - x^m) = \sum_{n=-\infty}^{\infty} (-1)^n x^{\omega(n)}$$

So, surprisingly, the LHS is a sort of generating function for the $\omega(n)$. Note also the surprising relationship between the $p(n)$ and $\omega(n)$:

$$1 = \left(\sum_{n=0}^{\infty} p(n)x^n \right) \left(\sum_{n=-\infty}^{\infty} (-1)^n x^{\omega(n)} \right)$$

Proof. (Euler by induction 1750, Legendre 1830, Jacobi 1846, Franklin 1881 gave this remarkable “combinatorial” proof) Let

$$\prod_{m=1}^{\infty} (1 - x^m) = 1 + \sum_{n=1}^{\infty} a(n)x^n$$

Now every partition of n into **unequal** parts produces a term on the right with

- +1 if x^n is the product of an **even** number of terms.
- -1 if x^n is the product of an **odd** number of terms.

Hence

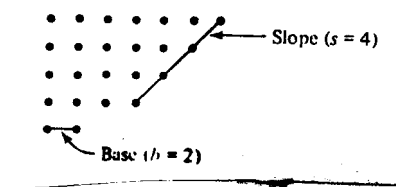
$$\prod_{m=1}^{\infty} (1 - x^m) = 1 + \sum_{n=1}^{\infty} (p_e(n) - p_o(n))x^n \quad (1)$$

Franklin showed that there is a 1-1 correspondence between even and odd partitions, so $p_e(n) = p_o(n)$, except when n is **pentagonal**.

Consider the graph of a partition. It is in **standard form** if the parts are in strictly **decreasing order** going down the page.

Definition The **base** of the graph is the longest line segment connecting points in the last row. Let b be the number of points.

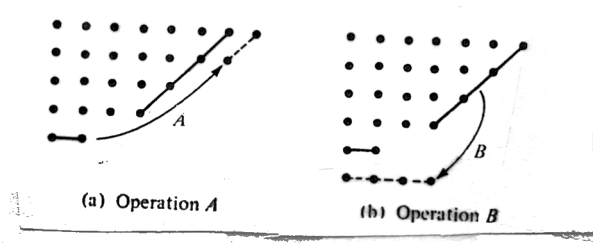
Definition The **slope** of the graph is the longest 45° segment joining the last point in the first row with the last point in successive rows. Let s be the number of points in the slope.



Definition Operation A: Move points on the base so they all lie on a line parallel to the slope. It is **permissible** if the resulting graph is in standard form.

Definition Operation B: Move all points on the slope so they lie on a line below the base. Again it is **permissible** if the resulting graph is in standard form.

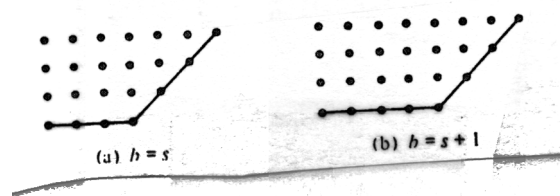
If A is permissible we get a **new** partition of n into unequal parts with **1 less** term. If B is permissible we get a **new** partition of n into unequal parts with **1 more** term.



If for a **given** n and **every** partition of n , exactly one of A or B is permissible, there will be a 1-1 correspondence between partitions of n into an even and odd number of terms $\Rightarrow p_e(n) = p_o(n)$ for these n .

Determination whether A or B is permissible:

- **Case 1** $b < s$: $b \leq s - 1 \Rightarrow$ A is okay but B is not.
- **Case 2** $b = s$: B is not okay. A is okay except when the base and slope intersect.



- **Case 3** $s < b$: A is **not** permissible, B is okay except when $b = s + 1$.

\therefore there are just two exceptions, (a) and (b) above.

- **Consider (a)**: Let there be k rows so $b = k$ and counting '•':s

$$n = k + (k + 1) + \dots + (2k - 1) = \frac{3k^2 - k}{2} = \omega(k)$$

So if k is even we get an *extra* partition into an even number (k) of parts. If K is odd we get an *extra odd* partition. $\therefore p_e(n) - p_o(n) = (-1)^k$.

- **In (b)**:

$$\begin{aligned} n &= \frac{3k^2 - k}{2} + k \text{ because there s an extra point on each row} \\ &= \frac{3k^2 + k}{2} \\ &= \omega(-k) \end{aligned}$$

and again $p_e(n) - p_o(n) = (-1)^k$.

Hence, by (1)

$$\prod_{m=1}^{\infty} (1 - x^m) = 1 + \sum_{k=1}^{\infty} (-1)^k x^{\omega(k)} + \sum_{k=1}^{\infty} (-1)^k x^{\omega(-k)}$$

□

Theorem (Euler) Let $P(0) = 1$ and $p(n) = 0$ for $n < 0$:

$$p(n) = \sum_{k=1}^{\infty} (1)^k \{p(n - \omega(k)) + p(n - \omega(-k))\}$$

Proof. By the above two theorems

$$\left(1 + \sum_{k=1}^{\infty} \{x^{\omega(k)} + x^{\omega(-k)}\}\right) \left(\sum_{m=0}^{\infty} p(m)x^m\right) = 1$$

For $n \geq 1$ the coefficient of x^n on RHS is zero. So equating coefficients of x^n on each side:

$$\begin{aligned} \sum_{n=0}^{\infty} p(n)x^n + \sum_{m=0}^{\infty} \sum_{k=1}^{\infty} (-1)^k p(m)x^{m+\omega(k)} + \sum_{m=0}^{\infty} \sum_{k=1}^{\infty} (-1)^k p(m)x^{m+\omega(-k)} &= 0 \\ \sum_{n=0}^{\infty} p(n)x^n + \sum_{n=0}^{\infty} \left[\sum_{k=1}^{\infty} (-1)^k p(n - \omega(k)) \right] x^n + \sum_{n=0}^{\infty} \left[\sum_{k=1}^{\infty} (-1)^k p(n - \omega(-k)) \right] x^n &= 0 \\ \Rightarrow p(n) = \sum_{k=1}^{\infty} (-1)^{k+1} \{p(n - \omega(k)) + p(n - \omega(-k))\} \end{aligned}$$

□

Ex $p(5) = \sum_{k=1}^{\infty} (-1)^{k+1} \{p(5 - \omega(k)) + p(5 - \omega(-k))\}$. Using $\omega(0) = 0$, $\omega(1) = 1$, $\omega(2) = 5$, $\omega(3) = 12$, $\omega(-1) = 2$, $\omega(-2) = 7$, $\omega(-3) = 15$. we get:

$$\begin{aligned} p(5) &= (-1)^2 \{p(5 - \omega(1)) + p(5 - \omega(-1))\} + (-1)^3 \{p(5 - \omega(2)) + p(5 - \omega(-2))\} \\ &= 1 \cdot \{p(4) + p(3)\} - \{p(0) + p(-2)\} + 0 \\ &= \{5 + 3\} - \{1 + 0\} \\ &= 7 \end{aligned}$$

as before.

An upper bound for p(n)

Theorem $\forall n \geq 1$, $p(n) < e^{k\sqrt{n}}$ where $k = \pi\sqrt{\frac{2}{3}}$.

Proof. Let $F(x) = \prod_{n=1}^{\infty} (1 - x^n)^{-1} = 1 + \sum_{k=1}^{\infty} p(k)x^k$ and restrict x to lie in $0 < x < 1$. Then $P(n)x^n < F(x)$, each term being positive. So

$$\begin{aligned} \log(p(n)) &< \log(F(x)) + n \log\left(\frac{1}{2}\right) \\ &= A + B \end{aligned}$$

First estimate A, then B:

$$\begin{aligned} A &= \log(F(x)) \\ &= -\log\left(\prod_{n=1}^{\infty} (1 - x^n)\right) \\ &= -\sum_{n=1}^{\infty} \log(1 - x^n) \\ &= \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{x^{mn}}{m} \\ &= \sum_{m=1}^{\infty} \frac{1}{m} \sum_{n=1}^{\infty} (x^m)^n \\ &= \sum_{m=1}^{\infty} \frac{1}{m} \cdot \frac{x^m}{1 - x^m} \end{aligned}$$

Now $\frac{1-x^m}{1-x} = 1 + x + x^2 + \dots + x^{m-1}$ and $0 < x < 1$ so

$$\begin{aligned} mx^{m-1} &< \frac{1 - x^m}{1 - x} < m \\ \Rightarrow \frac{m(1-x)}{x} &< \frac{1 - x^m}{x^m} < \frac{m(1-x)}{x^m} \end{aligned}$$

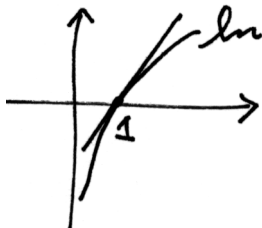
with all terms positive so inverting gives:

$$\frac{x^m}{m^2(1-x)} \leq \frac{1}{m} \cdot \frac{x^m}{1-x^m} \leq \frac{1}{m^2} \cdot \frac{x}{1-x}$$

Sum on m

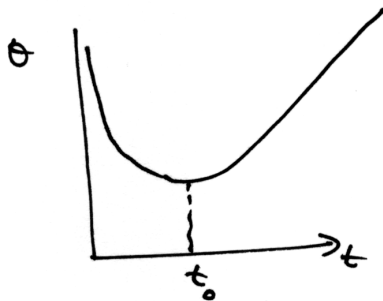
$$A = \sum_{m=1}^{\infty} \frac{1}{m} \cdot \frac{x^m}{1-x^m} \leq \frac{x}{1-x} \sum_{m=1}^{\infty} \frac{1}{m^2} = \frac{\pi^2}{6} \cdot \frac{x}{1-x}$$

Let $t = \frac{1-x}{x}$ so $1+t = 1 + \frac{1-x}{x} = \frac{1}{x}$ so $A \leq \frac{\pi^2}{6} \cdot \frac{1}{t}$ and $\log\left(\frac{1}{x}\right) = \log(1+t) < t$



Hence $\log(p(n)) < \log(F(x)) + n \log\left(\frac{1}{x}\right) < \frac{\pi^2}{6t} + nt$

Now the minimum value of $\theta(t) = \frac{\pi^2}{6t} + nt$ occurs when $t_0 = \frac{\pi}{\sqrt{6n}}$.



For this value of t

$$\theta(t_0) = 2nt_0 = \frac{2n\pi}{\sqrt{6n}} = K\sqrt{n}$$

Hence $\log(p(n)) < K\sqrt{n} \Rightarrow p(n) < e^{K\sqrt{n}}$. \square

We can use generating functions and **logarithmic differentiation** to devise recursion formulas for arithmetical functions:

Let $A \subset \mathbb{N}$ be a subset. Let $f(n)$ be an arithmetical function. Let the product

$$F_A(x) = \prod_{n \in A} (1 - x^n)^{-\frac{f(n)}{n}}$$

and the series

$$G_A(x) = \sum_{n \in A} \frac{f(n)}{n} x^n$$

converge absolutely for $|x| < 1$. Then

$$\begin{aligned} \log(F_A(x)) &= -\sum_{n \in A} \frac{f(n)}{n} \log(1 - x^n) \\ &= \sum_{n \in A} \frac{f(n)}{n} \sum_{m=1}^{\infty} \frac{x^{mn}}{m} \\ &= \sum_{m=1}^{\infty} \frac{1}{m} G_A(x^m) \end{aligned}$$

Then differentiate and multiply by x to obtain:

$$\begin{aligned}
 x \frac{F'_A(x)}{F_A(x)} &= \sum_{m=1}^{\infty} G'_A(x^m) x^m \\
 &= \sum_{m=1}^{\infty} \sum_{n \in A} f(n) x^{mn} \\
 &= \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} x_A(n) f(n) x^{mn} \\
 &= \text{RHS}
 \end{aligned}$$

where

$$x_A(n) = \begin{cases} 1 & n \in A \\ 0 & n \notin A \end{cases}$$

is the so-called **characteristic** function of A .

Now collect terms with $mn = k$ to get

$$\text{RHS} = \sum_{k=1}^{\infty} f_A(k) x^k$$

where

$$f_A(k) = \sum_{d|k} x(d) f(d) = \sum_{d|k, d \in A} f(d)$$

Hence

$$x F'_A(x) = F_A(x) \sum_{k=1}^{\infty} f_A(k) x^k \quad (1)$$

Now write $F_A(x)$ as a power series in x . The coefficient will depend on A and f of course so call them $p_{A,f}(n)$:

$$F_A(x) = \sum_{n=0}^{\infty} p_{A,f}(n) x^n, \quad p_{A,f}(0) = F_A(1) = \prod_{n \in A} 1 = 1$$

Finally, equate the coefficients of x^n on both sides of (1) to obtain

$$n p_{A,f}(n) = \sum_{k=1}^n f_A(k) p_{A,f}(n-k)$$

with

$$p_{A,f}(0) = 1 \text{ and } f_A(k) = \sum_{d|k, d \in A} f(d)$$

Ex $A = \mathbb{N}$, $f(n) = n \Rightarrow p_{A,f}(n) = p(n)$, the (unrestricted) **partition function**, and $f_A(k) = \sum_{d|k} d = \sigma(k)$; the **divisor sum** function so:

$$n p(n) = \sum_{k=1}^n \sigma(k) p(n-k)$$

Check: $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$, so LHS = 35

$$\begin{aligned}\text{RHS} &= \sigma(1)p(4) + \sigma(2)p(3) + \sigma(3)p(2) + \sigma(4)p(1) + \sigma(5)p(0) \\ &= 1 \cdot 5 + 3 \cdot 3 + 4 \cdot 2 + 7 \cdot 1 + 6 \cdot 1 \\ &= 35\end{aligned}$$