

PMath 340 - Elementary Number Theory

Benjamin Smith*

This is based on a course by Michael Rubinstein (Winter 2006). All errors are the responsibility of the author.

Contents

1	Bernoulli Polynomials	2
1.1	Euler-Maclaurin summation formula	2
1.2	Applications of Euler-Maclaurin approximation	4
1.3	Euler's constant	5
2	Divisibility and primes	6
2.1	Unique factorization	6
2.2	Application of unique factorization	7
2.3	Euclidean Algorithm	8
2.4	Riemann Hypothesis	10
2.5	Congruences	10
2.6	Application of arithmetic in congruence classes	10
2.7	Inverses modulo m	11
2.8	Euler's generalization of FLT	12
2.9	Chinese remainder theorem	14
3	Polynomial Congruences	14
3.1	Primitive roots and Quadratic residues	15
3.2	k^{th} power residues	16
3.3	Quadratic residues	18
3.4	Applications of Gauss' Lemma	20
3.5	Quadratic reciprocity	21
4	Continued fractions	22
4.1	Finite continued fractions	23
4.2	Infinite continued fractions	25
4.3	Pell's equations	29
5	Partitions	30

*Please send any corrections to bh2smith@gmail.com

1 Bernoulli Polynomials

The following three rules uniquely specify a sequence, $B_n(t)$, of polynomials.

1. $B_0(t) = 1$,
2. $B'_k(t) = kB_{k-1}(t)$ for $k \geq 1$ (i.e. $B_k(t) = \int_0^t B_{k-1}(x)dx + B_k(0)$), and
3. $\int_0^1 B_k(t)dt = 0$ for $k \geq 1$.

Proposition 1.1. For $k \geq 0$

$$\frac{B_{k+1}(t+1) - B_{k+1}(t)}{k+1} = t^k.$$

Proof. By induction on k . When $k = 0$, we have $B_1(t+1) - B_1(t) = t+1+1 - (t+1) = 1 = t^0$. Suppose now that the result holds for some $k > 0$ so that $\frac{B_{k+1}(t+1) - B_{k+1}(t)}{k+1} = t^k$. Now,

$$\begin{aligned} \frac{B_{k+2}(t+1) - B_{k+2}(t)}{k+2} &= \frac{k+2}{k+2} \left[\int_0^{t+1} B_{k+1}(x)dx - \int_0^t B_{k+1}(x)dx \right] + \frac{B_{k+2}(0) - B_{k+2}(0)}{k+2} \\ &= \underbrace{\int_0^1 B_{k+1}(x)dx}_{=0} + \int_1^{t+1} B_{k+1}(x)dx - \int_0^t B_{k+1}(x)dx \\ &= \int_0^t B_{k+1}(u+1)du - \int_0^t B_{k+1}(x)dx \\ &= \int_0^t (B_{k+1}(u+1) - B_{k+1}(u)) du \\ &= \int_0^t (k+1)u^k du = t^{k+1} \end{aligned}$$

as claimed. □

Note that

$$\sum_{i=1}^N i^k = \sum_{i=1}^N \left[\frac{B_{k+1}(i+1) - B_{k+1}(i)}{k+1} \right] = \frac{1}{k+1} (B_{k+1}(N+1) - B_{k+1}(1))$$

We use Big-Oh notation to simplify by approximating upper bounds (this is less precise than asymptotic). We say that f is *asymptotically equivalent* to g as $x \rightarrow a$ if $\lim_{x \rightarrow a} \frac{f(x)}{g(x)} = 1$ (denoted by $f \sim g$). Big-Oh notation is used as $x \rightarrow \infty$ and we say $f(x) = \mathcal{O}(g(x))$ if there exists x_0 such that $|f(x)| < cg(x)$ for some constant c and for all $x > x_0$. Also $f(x)$ is $\mathcal{O}(g(x))$ as $x \rightarrow a$ if $|f(x)| < cg(x)$ for some c for all $x \in B_\epsilon(a)$.

1.1 Euler-Maclaurin summation formula

is a method to approximate sums involving integers.

For instance, one may ask how well does the integral $\int_a^b g(x)dx$ approximate $\sum_{n=a+1}^b g(n)$? First notice that, assuming g' exists and is continuous on $[m, m+1]$,

$$g(m+1) = \int_m^{m+1} g(t)dt + \int_m^{m+1} (t-m)g'(t)dt.$$

Indeed, integrating the second term by parts gives,

$$\int_m^{m+1} (t-m)g'(t)dt = [(t-m)g(t)]_m^{m+1} - \int_m^{m+1} 1 \cdot g(t)dt = g(m+1) - \int_m^{m+1} g(t)dt.$$

Here, for $t \in [m, m+1]$ then $t-m$ is the fractional part of t . This is also found using the floor function $\lfloor t \rfloor$ which is the largest integer less than t so that the fractional part of t is given by $\{t\} = t - \lfloor t \rfloor$. Hence, we may alternatively express the above as

$$g(m+1) = \int_m^{m+1} g(t)dt + \int_m^{m+1} \{t\}g'(t)dt.$$

Now, adding these up gives

$$\sum_{m=a+1}^b g(m) = \int_a^b g(t)dt + \int_a^b \{t\}g'(t)dt$$

where $a, b \in \mathbb{Z}$, $a < b$ and assuming that g' exists and is continuous on $[a, b]$.

Further,

$$\begin{aligned} \int_a^b g(t)dt + \int_a^b \{t\}g'(t)dt &= \int_a^b g(t)dt + \frac{1}{2} \int_m^{m+1} g'(t)dt + \int_a^b (\{t\} - 1/2)g'(t)dt \\ &= \int_a^b g(t)dt + \frac{1}{2}[g(b) - g(a)] + \int_a^b B_1(\{t\})g'(t)dt. \end{aligned}$$

and subtracting $1/2$ makes $B_1(\{t\})$ smaller.

The above is called a *first order Euler-Maclaurin approximation*. Now consider

$$\int_a^b B_1(\{t\})g'(t)dt = \int_a^{a+1} B_1(\{t\})g'(t)dt + \int_{a+1}^{a+2} B_1(\{t\})g'(t)dt + \cdots + \int_{b-1}^b B_1(\{t\})g'(t)dt$$

whose typical term, via integration by parts, is

$$\begin{aligned} \int_m^{m+1} B_1(\{t\})g'(t)dt &= \frac{1}{2} [B_2(t-m)g'(t)]_m^{m+1} - \frac{1}{2} \int_m^{m+1} B_2(t-m)g''(t)dt \\ &= \frac{1}{2} [B_2(1)g'(m+1) - B_2(0)g'(m)] - \frac{1}{2} \int_m^{m+1} B_2(t-m)g''(t)dt \\ &= \frac{B_2(0)}{2} [g'(m+1) - g'(m)] - \frac{1}{2} \int_m^{m+1} B_2(t-m)g''(t)dt \end{aligned}$$

since $B_k(1) = B_k(0)$ for all $k \geq 2$. Now, inductively we can state the k^{th} order Euler-Maclaurin approximation as follows; Let $a, b \in \mathbb{Z}$ with $a < b$ and $g : \mathbb{R} \rightarrow \mathbb{R}$ so that $g^{(k)}$ exists and is continuous on $[a, b]$. Then

$$\sum_{m=a+1}^b g(m) = \int_a^b g(t)dt + \sum_{i=1}^k \frac{(-1)^i B_i(0)}{i!} [g^{(i-1)}(b) - g^{(i-1)}(a)] + \frac{(-1)^{k+1}}{k!} \int_a^b B_k(\{t\}) g^{(k)}(t) dt.$$

1.2 Applications of Euler-Maclaurin approximation

Proposition 1.2 (Stirling's formula for $n!$).

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

Proof. We have that $\log n! = \sum_{m=1}^n \log m = \sum_{m=2}^n \log m$ which, by first order E-M approximation is

$$\begin{aligned} \sum_{m=2}^n \log m &= \int_1^n \log(t)dt + \frac{1}{2}[\log n - \log 1] + \int_1^n \left[\frac{\{t\} - 1/2}{t} \right] dt \\ &= [t \log t - t]_1^n + \frac{\log n}{2} + \int_1^n \frac{\{t\} - 1/2}{t} dt \\ &= n \log n - n + 1 + \frac{\log n}{2} + \int_1^n \frac{\{t\} - 1/2}{t} dt \end{aligned}$$

so that

$$\log n! - (n \log n - n + 1 + \frac{1}{2} \log n) = 1 + \int_1^n \frac{\{t\} - 1/2}{t} dt \stackrel{H.W.}{=} \text{constant} + \mathcal{O}(1/n).$$

Hence, in the limit,

$$\lim_{n \rightarrow \infty} [\log n! - n \log n - n + 1 + \frac{1}{2} \log n] = C_1$$

and the exponential of this is $\lim_{n \rightarrow \infty} \frac{n!}{e^n \log n - n + 1/2 \log n} = C$. That is

$$\lim_{n \rightarrow \infty} \frac{n!}{n^n e^{-n} \sqrt{n}} = C$$

or that $n! \approx \left(\frac{n}{e}\right)^n \sqrt{n} \cdot C$.

The constant C here is called *Euler's constant* and is discussed next. □

1.3 Euler's constant

Consider the sum $\sum_{m=1}^N \frac{1}{m}$ which diverges as $N \rightarrow \infty$, but how quickly? Writing $1 + \sum_{m=2}^N 1/m$ so not to integrate near zero. Then

$$\begin{aligned} 1 + \sum_{m=2}^N 1/m &= 1 + \int_1^N \frac{dt}{t} + \frac{1}{2} \left[\frac{1}{N} - \frac{1}{1} \right] - \int_1^N \frac{\{t\} - 1/2}{t^2} dt \\ &= \log N + \frac{1}{2} + \frac{1}{2N} - \left[\int_1^\infty \frac{\{t\} - 1/2}{t^2} dt - \int_N^\infty \frac{\{t\} - 1/2}{t^2} dt \right]. \end{aligned}$$

Examining the bracketed terms one finds that $\int_1^\infty \frac{\{t\}-1/2}{t^2}$ is constant by comparison with $\int_1^\infty \frac{1}{t^2} dt$ and, furthermore, that $\left| \int_N^\infty \frac{\{t\}-1/2}{t^2} dt \right| \leq \frac{1}{2} \int_N^\infty \frac{1}{t^2} dt = \mathcal{O}(1/n)$. Hence then, the above evaluates as

$$\log N + \frac{1}{2} + \frac{1}{2N} - C + \mathcal{O}(1/N) = \log N + \gamma + \mathcal{O}(1/N)$$

where $\gamma = 0.5772\dots$ is *Euler's constant*.

Exercise 1.3. Prove that

1.

$$B_1(\{t\}) = \{t\} - 1/2 = -\frac{1}{\pi} \sum_{m=1}^{\infty} \frac{\sin(2\pi m + t)}{m} = \frac{-1}{\pi} \sum_{m \neq 0} \frac{e^{2\pi i m t}}{2\pi i m}$$

for $t \notin \mathbb{Z}$ and

2.

$$B_k(\{t\}) = -k! \sum_{m \neq 0} \frac{e^{2\pi i m t}}{(2\pi i m)^k}$$

for $t \in \mathbb{R}, k \geq 2$.

$B_k(\{t\})$ is continuous and even at $t \in \mathbb{Z}$. $B_2(1) = B_2(0)$, plugging in $t = 0$, let $k = 2k_0$ with $k_0 \geq 1$. Now $B_{2k_0}(0) = (-2k_0)! \sum_{m=-\infty, \neq 0}^{\infty} \frac{1}{(2\pi)^{2k_0} (-1)^{k_0} m^{2k_0}}$ so

$$\boxed{\sum_{m=1}^{\infty} \frac{1}{m^{2k_0}} = \frac{(-1)^{k_0+1} (2\pi)^{2k_0}}{(2k_0)!} \frac{1}{2} B_{2k_0}(0)}.$$

For example, if $k_0 = 1$ this is

$$\sum_{m=1}^{\infty} \frac{1}{m^2} = \frac{(2\pi)^2}{2!} \frac{1}{2} B_2(0) = \pi^2 B_2(0) = \pi^2/6$$

and if $k_0 = 2$ we have

$$\sum_{m=1}^{\infty} \frac{1}{m^4} = \frac{\pi^4}{90}.$$

2 Divisibility and primes

For integers $a, b \in \mathbb{Z}$, then a is said to be *divide* b if $b = ma$ for some $m \in \mathbb{Z}$. This is also written as $a|b$. Note that $0|0$ and $4|0$ but 0 does not divide 4 .

Some properties of divisibility are as follows; for $a, b, c \in \mathbb{Z}$

1. If $a|b$ and $b|c$ then $a|c$ (this is transitivity)
2. If $a|b$ and $b|c$ then $a|bx + cy$ for all $x, y \in \mathbb{Z}$
3. If $a|b$ and $b|a$ then $a = \pm b$
4. if $a|b$ and $b \neq 0$ then $|a| \leq |b|$

An integer $p \in \mathbb{Z}$ is said to be *prime* if its only positive divisors are 1 and p . Otherwise, p is said to be *composite*.

Lemma 2.1. *Any integer $n > 1$ is either prime, or a product of primes.*

Proof. By induction on n , this is true for $n = 2$ which is prime. Now assuming the result holds for all integers up to $n - 1$ and consider n . If n is prime, we are done. Otherwise n is not prime so there exists a positive divisor say $a \neq 1$. Now $n = ab$ for some $b \in \mathbb{Z}$ and we have that both $1 < a, b < n$. Now, by induction hypothesis, a and b are either prime or can be expressed as a product of primes. Thus, n can be expressed as a product of primes. $\square$

Theorem 2.2. *There are infinitely many primes.*

Proof. Let $2, 3, 5, 7, \dots, p$ be a list of primes $\leq p$. Consider $N := (2 \cdot 3 \cdot 5 \cdots p) + 1$. If 2 divides N then $2|N - (2 \cdot 3 \cdot 5 \cdots p) = 1$ which is not true. So $2 \nmid N$. Likewise, $3, 5, 7, \dots, p$ do not divide N . Our lemma implies that either N is prime or can be written as a product of primes, so there must be another prime in our list and this can always be done so there are infinitely many primes. $\square$

2.1 Unique factorization

Lemma 2.3. *Let $m \in \mathbb{Z}$ be ≥ 2 . Assume that m is uniquely expressible as a product of primes. If $p|m$ with p prime, then p must appear in the factorization of m .*

Proof. Let $p|m$ so that $m = p \cdot b$ for some $b \in \mathbb{Z}$. b is either prime, or expressible as a product of primes say $b = q_1 \cdots q_k$ with each q_i prime. So now $m = pq_1q_2 \cdots q_k$ is a unique factorization of m into primes which includes p . $\square$

Corollary 2.4. *If $m \geq 2$ is uniquely expressible as a product of primes with $p|m$ and $p'|m$ ($p \neq p'$), then pp' must appear in the factorization of m .*

Theorem 2.5 (Unique factorization of integers). *Every $n \in \mathbb{Z}$ ($n \geq 2$) is uniquely expressible as a product of primes.*

Proof. By induction; this hold for $n = 2$ which is prime. Now assuming the result holds for all numbers up to $n - 1$ and consider the n^{th} case. Assume that n has two distinct factorizations say $n = p_1 \cdots p_k = p'_1 \cdots p'_{k_2}$ where all the p_i, p'_j are prime and none of the primes on the left occur on the right (if so we could cancel). Without loss of generality $p_1 \leq p_2 \leq \cdots \leq p_k$ and $p'_1 \leq \cdots \leq p'_{k_2}$. We can assume n is composite since if it were prime, it would already be uniquely factorized. So both $k, k_2 \geq 2$ and $p_1^2, p'^2_1 \leq n$. Also assume without loss of generality that $p_1 < p'_1$ so $p_1 \leq p'_1 - 1$.

Now, $p_1 p'_1 \leq (p'_1 - 1) p'_1 = p'^2_1 - p'_1 \leq n - 2$ and hence $2 \leq n - p_1 p'_1 < n$. by induction hypothesis $n - p_1 p'_1$ is uniquely factorable and $p_1 | n$ so $p_1 | n - p_1 p'_1$. Also then $p'_1 | n - p_1 p'_1$ so our corollary (along with divisibility properties) implies that $p_1 p'_1 | n$ meaning that $n = p_1 p'_1 b$ for some $b \in \mathbb{Z}$. Let $b = q_1 \cdots q_l$ (be a product of primes) and now $n = p_1 p_2 \cdots p_k = p_1 p'_1 q_1 \cdots q_l$ allowing us to cancel p_1 and have two distinct factorizations of $n/p_1 < n$ (contradicting the induction hypothesis). $\square$

2.2 Application of unique factorization

Let $d(n)$ denote the number of divisors of n (positive). If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then

$$d(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1).$$

Now let $\sigma(n)$ denote the sum of the positive divisors of n . Then

$$\sigma(n) = \prod_{i=1}^k \left(\sum_{j=0}^{\alpha_i} p_i^j \right). \quad (1)$$

A map $f : \mathbb{Z}_{>0} \rightarrow \mathbb{C}$ is said to be *multiplicative* if $f(ab) = f(a)f(b)$ whenever $\gcd(a, b) = 1$. Note that both $d(n)$ and $\sigma(n)$ are multiplicative.

Indeed, let $n = \prod_{i=1}^k p_i^{\alpha_i}, m = \prod_{i=1}^l q_i^{\beta_i}$ be such that $\gcd(m, n) = 1$. Then

$$\sigma(nm) = \sigma \left(\prod_{i=1}^k p_i^{\alpha_i} \prod_{i=1}^l q_i^{\beta_i} \right) = \prod_{a=1}^k \left(\sum_{j=0}^{\alpha_j} p_a^j \right) \prod_{b=1}^l \left(\sum_{j=0}^{\beta_j} q_b^j \right) = \sigma(n)\sigma(m).$$

Observe that this does not hold when $\gcd(m, n) \neq 1$ (e.g. $\sigma(25) \neq \sigma(5)\sigma(5)$).

A *perfect number* n is a positive integer whose proper divisors sum to itself (i.e. $\sigma(n) = 2n$). The first two perfect numbers are 6 and 28.

Theorem 2.6. 1. *Euclid proved that if $n = 2^{k-1}p$ with $k \geq 2$ and $p = 2^k - 1$ is prime, then n is perfect.*

2. *Euler proved that if n is even and perfect then it is of the form $2^{k-1}p$ with $p = 2^k - 1$ prime.*

Proof. 1. Let $n = 2^{k-1}p$ with p an odd prime of the form $2^k - 1$. Then

$$\begin{aligned} \sigma(n) &= \sigma(2^{k-1})\sigma(p) = (1 + 2 + \cdots + 2^{k-1})(1 + p) \\ &= \frac{2^k - 1}{2 - 1}(1 + 2^k - 1) = (2^k - 1)2^k = 2n \end{aligned}$$

2. Let n be even and perfect (so that $n = 2^m \cdot n_0$ with n_0 odd and $m \geq 1$). Consider now,

$$\sigma(n) = \sigma(2^m)\sigma(n_0) = (2^{m+1} - 1)\sigma(n_0) = 2(2^m \cdot n_0) = 2^{m+1}n_0$$

since n is perfect. $2^{m+1} - 1$ is odd so by unique factorization theorem, $2^{m+1} | (2^{m+1} - 1)\sigma(n_0)$ which implies $2^{m+1} | \sigma(n_0)$. Thus $\sigma(n_0) = 2^{m+1}s$ for some $s \in \mathbb{Z}$ so $(2^{m+1} - 1)2^{m+1}s = 2^{m+1}n_0$ and hence $s | n_0$. Simplifying the previous equation says $2^{m+1}s = n_0 + s$ and we know $\sigma(n_0) = 2^{m+1}s$ which suggests¹ that n has two divisors. Hence n is prime and $s = 1$. Hence $n_0 = 2^{m+1} - 1$ (prime) and this verifies our claim. $\square$

Primes of the form $2^k - 1$ are called *Mersenne primes* however not all numbers of this form are prime. In fact, it remains an unsolved problem to verify whether or not there are infinitely many Mersenne primes (there probably are). Furthermore, none knows if there are any odd perfect numbers (probably not).

Theorem 2.7 (Division/Euclidean algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique integers q, r with $0 \leq r < b$ such that $a = qb + r$.*

Proof. Let $S = \{a - kb : k \in \mathbb{Z}\}$ and $T = \{m \in S : m \geq 0\}$. Observe first that T is non empty because $a - kb \geq 0$ whenever $k \leq a/b$ so infinitely many k work. Now, T is comprised of non-negative integers and any non-empty set of non-negative integers has a minimal element (this is by the well-ordering principal which is equivalent to the axiom of choice). Let r be the minimal element in T and q the corresponding k . By these means, we have that $a - qb = r$ with $r \geq 0$. We seek to show that $r < b$, so assume for the moment that $r \geq b$. If this were the case, then $r - b = a - (q + 1)b > 0$ and is in S so $a - (q + 1)b \in T$ and is smaller than r (contradicting minimality of r).

We have non shown existence of q and r but remain to verify the uniqueness. For this, suppose that $a = q_1b + r_1 = q_2b + r_2$ with both $0 \leq r_1, r_2 < b$. Equivalently, then $0 = (q_1 - q_2)b + (r_1 - r_2)$ which implies $(q_2 - q_1)b = (r_1 - r_2)$ and hence $b | (r_1 - r_2)$. However, $-b < -r_2 \leq r_1 - r_2 \leq r_1 < b$ so $r_1 - r_2 = 0$ which implies $r_1 = r_2$ and $q_1 = q_2$ hence, uniqueness. $\square$

Let $a, b \in \mathbb{Z}$, an integer c is called a *common divisor* of a and b if both $c | a$ and $c | b$. Define the $\gcd(a, b)$ to be the greatest common divisor of a and b

2.3 Euclidean Algorithm

This algorithm is used to find the greatest common divisor of two integers and is essentially a repeated division algorithm until the remainder is zero. We claim that remainders are strictly decreasing, non-negative and hence must reach 0. Furthermore, the $\gcd(a, b)$ is preserved on every line.

Indeed, let $d = \gcd(a, b)$ so that $d | a, b$ hence $d | a - qb = r$ so that d is a common divisor of both b and r . To see that it is furthermore the greatest common divisor of b and r , let c be any other common divisor and show $c \leq d$. We have $c | b$ and $c | r$ so $c | qb + r = a$, hence c is a common divisor of b and a so is $\leq d$.

¹although I think this should be verified

Lemma 2.8. *If $d = \gcd(a, b)$ then there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$ (and any multiple of d).*

This follows from back substitution of the Euclidean algorithm

Example 2.9. Let $a = 527, b = 153$. Then

$$\begin{aligned} 527 &= 3 \cdot 153 + 68 \\ 153 &= 2 \cdot 68 + 17 \\ 68 &= 4 \cdot 17 + 0 \end{aligned}$$

so $\gcd(a, b) = 17$ and applying this algorithm backwards, we get

$$17 = 153 - 2 \cdot 68 = 153 - 2(527 - 3 \cdot 153) = 7 \cdot 153 - 2 \cdot 527.$$

Theorem 2.10. *Let $a, b, c \in \mathbb{Z}$ and assume that $a|bc$ but $\gcd(a, b) = 1$. Then $a|c$*

Proof. $\gcd(a, b) = 1$ implies that there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiplying this by c gives $acx + bcy = c$. Now $a|ac$ and $a|bc$ (by assumption) so $a|acx + bcy = c$ as required. $\square$

Corollary 2.11. *Let p be prime $b, c \in \mathbb{Z}$ and let $p|bc$. If $p \nmid b$ then $p|c$. Furthermore, if $p|b_1b_2B - 3 \cdots b_k$ then $p|b_i$ for some i .*

Proof. If $p \nmid b$ then $\gcd(p, b) = 1$ and this is precisely the conditions required from the previous theorem. $\square$

With these results, one may provide an inductive proof of the unique factorization theorem as follows; Suppose $n \geq 2$ has two distinct factorizations $p_1 \cdots p_k = p'_1 \cdots p'_l$. We have $p_1|n = p'_1 \cdots p'_l$ so then $p_1|p'_j$ for some j . This implies $p_1 = p'_j$ so they may be canceled. Repeating this indefinitely one finds that all of the prime factors of n coincide and we are done.

One may apply unique factorization to give Euler's proof that there are infinitely many primes. Let $s > 1$ and consider

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \prod_{\forall p} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots \right).$$

By unique factorization, every $n \in \mathbb{N}$ appears exactly once and his series is absolutely convergent since $s > 0$ so rearranging sums is valid. Hence,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\forall p} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots \right) = \prod_{\forall p} \frac{1}{1 - 1/p^s}.$$

Now, Euler substitutes the value $s = 1$ so that the left hand side diverges (as the Harmonic series), so the right hand side must have infinitely many factors (in order to diverge).

How many primes are there? Let $\pi(x)$ denote the number of primes $\leq x$. For example, $\pi(10^6) = 78498$.

Gauss conjectured that at x , the average gap size between primes is approximately $\log x$. That is to say the density of primes near x is $\frac{1}{\log x}$, so Gauss conjectured that $\pi(x) \approx \int_2^x \frac{dt}{\log t} = \frac{x}{\log x}$ so that $\pi(x) \approx \frac{x}{\log x}$. This was proven in 1896.

2.4 Riemann Hypothesis

$$\pi(x) = \int_2^x \frac{dt}{\log t} + \mathcal{O}(x^{1/2} \log x) = \frac{x}{\log x} + \mathcal{O}(\sqrt{x} \log x).$$

To demonstrate an example, we have $\pi(10^{13}) = 346,065,536,839$ and $\frac{10^{13}}{\log 10^{13}} = 108971$.

2.5 Congruences

Let $a, b, m \in \mathbb{Z}$ with $m \geq 1$. we say that a is *congruent* to b modulo m (i.e. $a \equiv b \pmod{m}$) if $m|a - b$. Note that $a \equiv b \pmod{m}$ if and only if they both have the same remainder when divided by m . Indeed, let $a = km + r$ and $b = lm + s$ with $0 \leq r, s < m$. If $r = s$ then $m|a - b = (k - l)m$ and if $m|a - b = (k - l)m + (r - s)$ then also $m|r - s$ so $r - s = c \cdot m$ for some integer c , but the constraint that $0 \leq r, s < m$ implies $c = 0$ so $r = s$.

Note that the only possible remainders modulo m are $0, 1, 2, \dots, m - 1$ and these integers form a complete set of residues (i.e. any integer is congruent to exactly one of these (modulo m)).

Lemma 2.12. *Congruence is an equivalence relation (i.e. 1. $a \equiv a \pmod{m}$ 2. if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$ and 3. if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$).*

Proof. We only prove 3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $m|a - b$ and $m|b - c$ so $m|a - b + b - c = a - c$ as required. $\square$

Lemma 2.13. *Let $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then $a + b \equiv a' + b' \pmod{m}$ and $ab \equiv a'b' \pmod{m}$.*

Proof. This is trivial from definition (i.e. tautological). $\square$

The addition rule for congruence classes holds and includes subtraction. What about division? We check if $ca \equiv cb \pmod{m}$ then $m|c(a - b)$ and if $\gcd(c, m) = 1$ then $m|a - b$ so $a \equiv b \pmod{m}$. However, if $\gcd(c, m) \neq 1$ then we may not have division.

For example, $3 \cdot 1 \equiv 3 \cdot 3 \pmod{6}$ but $1 \not\equiv 3 \pmod{6}$.

2.6 Application of arithmetic in congruence classes

How can one tell if an integer is divisible by 9? Write $n = \sum_{k=0}^N a_k \cdot 10^k$ with each $a_i \in \{0, \dots, 9\}$. Now, since $10 \equiv 1 \pmod{9}$ then $n \equiv \sum_{k=0}^N a_k \pmod{9}$. Hence,

$$9|n \text{ if and only if } 9|\sum_{k=0}^N a_k.$$

2.7 Inverses modulo m

Let $m \in \mathbb{Z}$, $m \geq 1$. An element $a \in \mathbb{Z}$ is said to have an *inverse* modulo m if there exists $b \in \mathbb{Z}$ such that $a \cdot b \equiv 1 \pmod{m}$. If such a b exists, it is denoted by a^{-1} .

Lemma 2.14. *a is invertible modulo m if and only if $\gcd(a, m) = 1$.*

Proof. If a is invertible modulo m then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$ so that $m \mid ab - 1$ meaning $ab - 1 = km$ for some $k \in \mathbb{Z}$. Let $d = \gcd(a, m)$ so $d \mid a$ and $d \mid m$ hence $d \mid ab - km = 1$. Thus $d = 1$.

Conversely, if $\gcd(a, m) = 1$ so there exists $x, y \in \mathbb{Z}$ such that $ax + my = 1$ (by Euclidean algorithm) so $ax - 1 = -my$ which means $m \mid ax - 1$ and thus $ax \equiv 1 \pmod{m}$. $\square$

Example 2.15. Find $20^{-1} \pmod{93}$. Applying the Euclidean algorithm;

$$93 = 4 \cdot 20 + 13$$

$$20 = 1 \cdot 13 + 7$$

$$13 = 1 \cdot 7 + 6$$

$$7 = 1 \cdot 6 + 1$$

$$6 = 6 \cdot 1 + 0$$

Now, back substitution gives

$$\begin{aligned} 1 &= 7 - 1 \cdot 6 \\ &= 7 - (13 - 7) \\ &= 2 \cdot 7 - 13 \\ &= 2(20 - 13) - 13 \\ &= 2(20) - 3 \cdot 13 \\ &= 2(20) - 3(93 - 4 \cdot 20) \\ &= 14(20) - 3(93) \end{aligned}$$

so $20^{-1} = 14$.

Another further application of this allows us to solve linear congruences modulo m . For example, solve $20x \equiv 7 \pmod{93}$. Multiplying by $20^{-1} = 14$ gives $x \equiv 14 \cdot 7 \equiv 5 \pmod{93}$. Note that $ax \equiv b \pmod{m}$ is called a *linear congruence*.

alternative proof for inverses; Let $\gcd(a, m) = 1$. and consider the set of integers $0 \cdot a, 1 \cdot a, \dots, (m-1) \cdot a$. These are all distinct modulo m so one of them must be congruent to 1 modulo m . Indeed, for two to be equal (mod m) then $b_1 a \equiv b_2 a \pmod{m}$ so that $m \mid a(b_1 - b_2)$, but $\gcd(a, m) = 1$ so $m \mid b_1 - b_2$ which means $b_1 \equiv b_2 \pmod{m}$. However, $-(m-1) \leq b_1 - b_2 \leq m-1$ which implies $b_1 = b_2$. $\square$

Example 2.16. Let $m = 12$ and $a = 5$ so that $\gcd(a, m) = 1$. Consider the set $0 \cdot 5, 1 \cdot 5, \dots, 11 \cdot 5$ which is $0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7$ and we find that $5^{-1} = 5$.

Theorem 2.17 (Fermat's little theorem). *Let p be prime and $a \in \mathbb{Z}$ such that p does not divide a . Then $a^{p-1} \equiv 1 \pmod{p}$. Also $a^p \equiv a \pmod{p}$ even if p does divide a .*

Proof. Consider the set $1 \cdot a, 2 \cdot a, \dots, (p-1) \cdot a$ which are all distinct modulo p . Also, none are congruent to zero. This is because $p|b \cdot a$ implies $p|b$ since p does not divide a and $1 \leq b \leq p-1$ which implies p does not divide b so p can't divide ba . So $a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$. This implies that $p|(a^{p-1})(1 \cdot 2 \cdot 3 \cdots (p-1))$, but $\gcd(p, 1 \cdot 2 \cdot 3 \cdots (p-1)) = 1$ so $p|a^{p-1} - 1$ as required. $\square$

2.8 Euler's generalization of FLT

Let $\varphi(m)$ denote the number of integers $0 \leq c \leq m$ such that $\gcd(c, m) = 1$.

Example 2.18. $\varphi(12) = 4$ and $\varphi(15) = 8$ having coprime c 's $\{1, 5, 7, 11\}$ for 12 and $\{1, 2, 4, 7, 8, 11, 13, 14\}$ for 15.

An integer $c = qm + r$ with $0 \leq r < m$ has $\gcd(c, m) = 1$ if and only if $\gcd(r, m) = 1$. This says that the remainder specifies whether a number has a common factor with m or not. Let $c_1, c_2, \dots, c_{\varphi(m)}$ be distinct integers satisfying that $0 \leq c_i < m$ with $\gcd(c_i, m) = 1$. Let $\gcd(a, m) = 1$ and consider the collection $ac_1, ac_2, \dots, ac_{\varphi(m)}$. These are all distinct modulo m and furthermore $\gcd(ac_i, m) = 1$ so the product $\prod ac_i \equiv \prod c_i \pmod{m}$ which means (again) that $m|(a^{\varphi(m)} - 1) \prod c_i$, but the $\gcd(\prod c_i, m) = 1$ so in fact $m|a^{\varphi(m)} - 1$. Hence, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Theorem 2.19 (Euler's generalization of FLT). *Let $a, m \in \mathbb{Z}$ with $m \geq 1$ and $\gcd(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$ where $\varphi(m) = \{0 \leq c < m : \gcd(c, m) = 1\}$.*

Example 2.20. If $m = 15$ and $a = 4$ then

$$(1 \cdot 4)(2 \cdot 4)(4 \cdot 4)(7 \cdot 4)(8 \cdot 4)(11 \cdot 4)(13 \cdot 4)(14 \cdot 4) \equiv 1 \cdot 2 \cdot 4 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 14 \pmod{15}$$

$$4^8 \equiv 1 \pmod{15}$$

Some formulas for the *Euler-phi function* are given as follows

Proposition 2.21. 1. *If p is prime, then $\varphi(p) = p - 1$.*

2. *If p is prime and $\alpha \in \mathbb{N}$ then $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - 1/p)$.*

3. *Let p, q be distinct primes, then $\varphi(pq) = pq - p - q + 1$.*

4. *Let a, b be coprime integers, then $\varphi(ab) = \varphi(a)\varphi(b)$.*

proof (of 4.) First by illustration when $a = 6, b = 5$ write all of the numbers from 0 to $ab - 1 = 29$ in a block as

0	6	12	18	24
1	7	13	19	25
2	8	14	20	26
3	9	15	21	27
4	10	16	22	28
5	11	17	23	29

and notice that 6 divides the first row, 2 divides the third, 3 divides the fourth and 2 divides the fifth. So only the second and sixth rows are any good. This means, if $0 \leq m \leq 29$ then 20 are immediately pulled out as having $\gcd(m, 30) = 1$. Looking at the remaining two rows modulo $b = 5$. Row 2 becomes 1, 2, 3, 4, 0 and of these five $\varphi(5) = 4$ work. The sixth row becomes 0, 1, 2, 3, 4 and again $\varphi(5) = 4$ work. We now have $2 = \varphi(a)$ rows each providing $4 = \varphi(5)$ valid m 's.

To generalize the above illustration, write

$$\begin{array}{ccccccc} 0 & a & 2a & \cdots & (b-1)a & & \\ 1 & a+1 & \cdots & & \vdots & & \\ 2 & & & & & & \\ \vdots & & & & & & \\ a-1 & 2a-1 & \cdots & & \underbrace{(b-1)a+a-1}_{=ab-1} & & \end{array}$$

Recall that if $m = qa + r$ with $0 \leq r < m$ then $\gcd(a, m) = \gcd(a, r)$. Our goal is to pick out the m 's in $0 \leq m < ab$ such that $\gcd(m, ab) = 1$ which holds if and only if both $\gcd(m, a) = 1$ and $\gcd(m, b) = 1$. This says, that we may restrict ourselves to $\varphi(a)$ rows beginning with r such that $\gcd(r, a) = 1$. Next take a given row $r, a+r, 2a+r, \dots, (b-1)a+r$. Modulo b , this row forms a complete set of residues. So of these, exactly $\varphi(b)$ are coprime with b . All together this is

$$\varphi(ab) = \underbrace{\varphi(a)}_{\text{valid rows}} \cdot \underbrace{\varphi(b)}_{\text{valid number per row}}.$$

□

Making use of all of the above properties, then with $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$$\varphi(n) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k p_i^{\alpha_i} (1 - 1/p_i) = n \cdot \prod_{p|n} (1 - 1/p).$$

Proposition 2.22.

$$\sum_{d|n} \varphi(d) = n$$

Proof. Making use of Equation (1),

$$\begin{aligned} \sum_{d|n} \varphi(d) &= \prod_{i=1}^k (1 + \varphi(p_i) + \varphi(p_i)^2 + \cdots + \varphi(p_i)^{\alpha_i}) \\ &= \prod_{i=1}^k (1 + (p_i - 1) + p_i(p_i - 1) + \cdots + p_i^{\alpha_i-1}(p_i - 1)) \\ &= \prod_{i=1}^k \left(1 + (p_i - 1) \cdot \frac{p_i^{\alpha_i} - 1}{p_i - 1} \right) = \prod_{i=1}^k p_i^{\alpha_i} = n. \end{aligned}$$

□

2.9 Chinese remainder theorem

Theorem 2.23 (Chinese remainder theorem). *Let $a, b \in \mathbb{Z}$ both ≥ 1 and $\gcd(a, b) = 1$. Given $\alpha, \beta \in \mathbb{Z}$ we can find an integer x such that $x \equiv \alpha \pmod{a}$ and $x \equiv \beta \pmod{b}$. Furthermore, the solution is unique if we restrict x to be $0 \leq x \leq ab$. In other words, two simultaneous congruences $x \equiv \alpha \pmod{a}$ and $x \equiv \beta \pmod{b}$ are equivalent to a single congruence modulo ab .*

This theorem allows us to simplify the above prove that $\gcd(a, b) = 1$ implies $\varphi(ab) = \varphi(a)\varphi(b)$. Indeed, Let $m \equiv r_1 \pmod{a}$ and $m \equiv r_2 \pmod{b}$ with $0 \leq r_1 < a$ and $0 \leq r_2 < b$. Now $\gcd(m, ab) = 1$ if and only if both $\gcd(m, a) = \gcd(m, r_1) = 1$ and $\gcd(m, b) = \gcd(r_2, b) = 1$ of which there are $\varphi(a)$ and $\varphi(b)$ possibilities respectively. By the Chinese Remainder Theorem (CRT), each pair (r_1, r_2) provides a unique $0 \leq m \leq ab$ satisfying the conditions $m \equiv r_1 \pmod{a}$ and $m \equiv r_2 \pmod{b}$. Thus there are all together $\varphi(a)\varphi(b)$ pairs so demonstrating our claimed result.

Theorem 2.24 (Wilson's Theorem). *Let p be prime, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Matching up inverse pairs $1, 2, 3, 4, \dots, (p-1)$ are all invertible modulo p since non share common factors with p . Most of them are not equal to their own inverse². Hence then, by matching inverse pairs,

$$(p-1)! \equiv 1 \cdot (p-1) \equiv (p-1) \pmod{p}.$$

□

3 Polynomial Congruences

Theorem 3.1 (Lagrange's Theorem). *Let p be prime, $n \in \mathbb{Z}$ non negative and $a_i \in \mathbb{Z}$ with $a_n \not\equiv 0 \pmod{p}$. Then the polynomial equation*

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$$

has at most n solutions modulo p .

Proof. By induction on n ; This holds for $n = 0$ since $a_0 \equiv 0$ has no solutions. Furthermore, this is true when $n = 1$ since $a_1 x + a_0 \equiv 0 \pmod{p}$ has one solution $x \equiv a_1^{-1} a_0 \pmod{p}$.

For the inductive step, the slick way is to use long division to pull out a linear factor for each root. Either $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$ has a root or not. If not, then zero roots is less than n as claimed. If there is a root, say x_1 , then the difference between our original equation from the and the same one with x_1 substituted for x is $a_n(x^n - x_1^n) + \dots + a_1(x - x_1) = 0$ which factors as $(x - x_1) \cdot g(x) \equiv 0 \pmod{p}$ where g has integer coefficients and $\deg g = n - 1$. Now, $p \mid (x - x_1) \cdot g(x)$ which implies $p \mid (x_1)$ or $g(x)$ (since p is prime). Hence, by induction hypothesis there are at most one plus $n - 1$ solutions modulo p . □

Example 3.2. 1. $x^3 - x \equiv 0 \pmod{3}$ has 3 solutions $x \equiv 0, 1, 2 \pmod{3}$.

²for this, one requires $a^2 \equiv 1 \pmod{p} \Rightarrow p \mid a^2 - 1 = (a+1)(a-1)$ so that $a \equiv \pm 1 \pmod{p}$

2. $x^3 + 1 \equiv 0 \pmod{3}$ has 1 solution modulo 3 and that is $x \equiv 2 \pmod{3}$.
3. A counter example in the case that p is not prime; $x^2 - 1 \equiv 0 \pmod{8}$ has 4 (> 2) solutions. These are $x \equiv 1, 3, 5, 7 \pmod{8}$.

3.1 Primitive roots and Quadratic residues

Let $m \in \mathbb{Z}$ be positive and $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. The *order* of a modulo m is the smallest possible integer l such that $a^l \equiv 1 \pmod{m}$.

Theorem 3.3 (Euler's Theorem). *If $\gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod{m}$ which implies that the order of a is $\leq \varphi(m)$.*

Example 3.4. $m = 11$ and $\varphi(m) = 10$.

Observe that	$1^1 \equiv 1 \pmod{11}$	$6^{10} \equiv 1 \pmod{11}$
	$2^{10} \equiv 1 \pmod{11}$	$7^{10} \equiv 1 \pmod{11}$
	$3^5 \equiv 1 \pmod{11}$	$8^{10} \equiv 1 \pmod{11}$
	$4^5 \equiv 1 \pmod{11}$	$9^5 \equiv 1 \pmod{11}$
	$5^5 \equiv 1 \pmod{11}$	$10^2 \equiv 1 \pmod{11}$

and these exponents are all divisors of $\varphi(m) = 10$.

Proof. Let $\gcd(a, m) = 1$ and suppose l is the order of a . We have $a^l \equiv 1 \pmod{m}$, but $a^i \not\equiv 1 \pmod{m}$ for all $0 < i < l$. We wish to show that $l | \varphi(m)$. Let $\varphi(m) = ql + r$ with $0 \leq r < l$ and show that $r = 0$. By Euler's Theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$ meaning that $a^r \equiv 1 \cdot a^r \equiv (a^l)^q \cdot a^r \equiv a^{ql+r} \equiv a^{\varphi(m)} \equiv 1$. Thus, as already noted, we must have $r = 0$ so that $l | \varphi(m)$ as required. $\square$

Furthermore, if a is known to have order l modulo m (and $\gcd(a, m) = 1$) then $a^k \equiv 1 \pmod{m}$ if and only if l divides k . This holds for the same reason as the previous result.

Lemma 3.5. *Let j be a positive integer. If a has order l , then a^j has order $l / \gcd(l, j)$.*

Proof. Order of a^j is the smallest integer k such that $(a^j)^k = (a^j)^k \equiv 1 \pmod{m}$, hence if and only if $l | jk$. Let $d = \gcd(j, l)$ so that $j = dj_0$ and $l = dl_0$ with $\gcd(j_0, l_0) = 1$. Now $l | jk$ implies $dl_0 | dj_0k$ or, equivalently, $l_0 | j_0k$ meaning $j_0k = \alpha l_0$ and so $k = \frac{\alpha l_0}{j_0}$. But k is an integer so we must have that $j_0 | \alpha l_0$ which means $j_0 | \alpha$. Thus, the smallest positive k has $\alpha = j_0$ which implies $k = l_0 = l/d$ as claimed. $\square$

An integer $a \in \mathbb{Z}$ is said to be a *primitive root* modulo m if its order equals $\varphi(m)$. Not all moduli have primitive roots (e.g. $m = 8$ since $1^2 = 3^2 = 5^2 = 7^2 \equiv 1 \pmod{8}$ and $\varphi(8) = 4$).

We claim that m has a primitive root if and only if $m = 2, 4, p^\alpha$ or $2p^\alpha$ where p is any odd prime and $\alpha \geq 1$. We shall demonstrate only that primes have primitive roots. For example, when $p = 11$, the primitive roots are 2, 6, 7 and 8.

We have seen that if a has order l modulo p , then $l \mid \varphi(p) = p - 1$. Let $f_p(l) = \#\{1 \leq a \leq p - 1 : a^l \equiv 1 \pmod{p}\}$ and notice that $\sum_{l \mid p-1} f_p(l) = p - 1$ which counts the number of a 's according to their order.

We claim that

1. If $l \mid p - 1$ then $f(l) \leq \varphi(l)$, and
2. claim 1 implies $f(l) = \varphi(l)$.

To show the second, assume that $f(l) \leq \varphi(l)$ so that

$$p - 1 = \sum_{l \mid p-1} f_p(l) \leq \sum_{l \mid p-1} \varphi(l) = p - 1.$$

Now, for the first claim, either $f(l) = 0$ or not, if $f(l) = 0$ then $f(l) \leq \varphi(l)$. If $f(l) \neq 0$ then there is at least one a with $1 \leq a \leq p - 1$ with order l and $a^j \not\equiv 1 \pmod{p}$ for all $j \in \{1, 2, \dots, l - 1\}$. Now consider the equation $x^l - 1 \equiv 0 \pmod{p}$. a is a solution to this equation and so are $a^2, a^3, \dots, a^l$ since $(a^j)^l - 1 = (a^l)^j - 1 \equiv 0 \pmod{p}$. Since a has order l , all of these a^j 's are distinct modulo p so we have found all solutions to this degree l equation (Lagrange's Theorem). Our goal then is to determine $f(l)$ (i.e. how many elements have order l).

Check how many of $a, a^2, a^3, \dots, a^l$ have order l . If a has order l , then a^j has order $l / \gcd(j, l)$ implying that $\varphi(l)$ of the j 's satisfy $\gcd(j, l) = 1$. Thus, if $f(l) \neq 0$ then $f(l) = \varphi(l)$. In particular, the number of primitive roots modulo p is precisely $\varphi(p - 1)$.

Let g be a primitive root modulo p ; then $g, g^2, g^3, \dots, g^{p-1}$ are congruent to $1, 2, 3, \dots, p - 1$ mod p only they're in some strange order.

Note that the primitive roots modulo 11 are 2, 6, 7, 8 and there are $\varphi(10) = \varphi(2) \cdot \varphi(5) = (2 - 1)(5 - 1) = 4$ of them. So $2, 2^2, 2^3, \dots, 2^9, 2^{10}$ equal to $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$ respectively.

3.2 k^{th} power residues

An integer a is said to be a k^{th} power residue modulo p if there exists some integer $x \in \mathbb{Z}$ such that $x^k \equiv a \pmod{p}$. Otherwise, a is a k^{th} power non-residue mod p . Note that we do not consider $a \equiv 0 \pmod{p}$.

Example 3.6. The quadratic residues modulo 11 are found from the following table;

1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2
1	4	9	5	3	3	5	9	4	1

Hence 1, 3, 4, 5, 9 are quadratic residues.

In terms of our primitive root, $g = 2$, all quadratic residues are of the form g^{2m} with $m = 1, 2, 3, 4, 5$.

Let g be a primitive root modulo p and rewrite $x^k \equiv a \pmod{p}$ in terms of g as follows; $a = g^\alpha$ and $x = g^\lambda$ for some $\alpha, \lambda \in \{1, 2, \dots, p - 1\}$. The congruence then becomes $(g^\lambda)^k \equiv g^\alpha \pmod{p}$ which is equivalent to $\lambda k \equiv \alpha \pmod{p - 1}$ which can be solved if and only if $\gcd(k, p - 1)$ divides α .

Note that $ax \equiv b \pmod{m}$ has solutions if and only if $\gcd(a, m) | b$. Indeed, let $d = \gcd(a, m)$ and if $d | b$ then the original equation is equivalent to $(a/d)x \equiv b/d \pmod{m/d}$. A solution to this equation (modulo m/d) gives rise to d solutions modulo m of the original equation. We have then solutions above if and only if $\gcd(k, p-1) | \alpha$. If so, then there are d solutions modulo $p-1$ to our equation. $x^2 \equiv a \pmod{11}$ if and only if $\lambda \cdot 2 \equiv \alpha \pmod{11-1=10}$. $\gcd(2, 10) = 2$ which implies $2 | \alpha$ for $1 \leq \alpha \leq 10$ so $10/2 = 5$ of the α 's are quadratic residues.

Let p be a prime and g a primitive root modulo p . You can write any $1 \leq a \leq p-1$ as $a \equiv g^\alpha \pmod{p}$ for some $1 \leq \alpha \leq p-1$. This α is called the *index* of a relative to the primitive root $g \pmod{p}$. α is uniquely specified if we restrict it to $1 \leq \alpha \leq p-1$ as powers of $g \pmod{p}$ repeat every $p-1$ (since g has order $p-1$). Now, $g^{\alpha'} \equiv g^\alpha \pmod{p}$ which is equivalent to $\alpha' = m(p-1) + \alpha$ which implies $\alpha' \equiv \alpha \pmod{p-1}$. Indeed, $\alpha' = m(p-1) + \alpha$ implies $g^{\alpha'} \equiv g^{m(p-1)+\alpha} \equiv (g^{p-1})^m \cdot g^\alpha \equiv g^\alpha \pmod{p}$. Conversely, if $\alpha' = m(p-1) + r$ with $1 \leq r \leq p-1$ (where $r = 0$ is not important). then $g^{\alpha'} = g^{m(p-1)+r} \equiv (g^{p-1})^m \cdot g^r \equiv g^r \pmod{p}$. If $g^{\alpha'} \equiv g^\alpha \pmod{p}$ then $g^r \equiv g^\alpha$ so that $r = \alpha$ because the powers of g do not repeat with the constraint $1 \leq r, \alpha \leq p-1$.

Example 3.7. $g = 3$ is a primitive root mod 7.

3	3 ²	3 ³	3 ⁴	3 ⁵	3 ⁶
3	2	6	4	5	1

The primitive roots mod 11 are 2, 6, 7, 8 powers of 2 are

2	2 ²	2 ³	2 ⁴	2 ⁵	2 ⁶	2 ⁷	2 ⁸	2 ⁹	2 ¹⁰	2 ¹¹	2 ¹²
2	4	8	5	10	9	7	3	6	1	2	4

The a 's which are quadratic residues modulo 11 are 1, 3, 4, 5, 9. If you didn't know about primitive roots then you could square all of the integers mod 11.

If $x^2 \equiv a \pmod{p}$ then $(p-x)^2 \equiv (-x)^2 \equiv x^2 \equiv a \pmod{p}$. So quadratic residues, if any always occur in pairs x and $p-x$.

Example 3.8. Cubic residue modulo 11. $x^3 \equiv a \pmod{11}$ in terms of primitive root g . Let $x = g^\lambda$ and $a \equiv g^\alpha$ then $g^{3\lambda} \equiv g^\alpha \pmod{p}$ means that $3\lambda \equiv \alpha \pmod{p-1}$. Here $p = 11$ so we want $3\lambda \equiv \alpha \pmod{10}$. $\gcd(3, 10) = 1$ and $1 | \alpha$ for all $\alpha = 1, 2, \dots, 10$. Hence all such α are cubic residues mod 11.

Check;

x	1	2	3	4	5	6	7	8	9	10
x^3	1	8	5	9	4	7	2	6	3	10

Lets now take a look at 5th power residues mod 11. Again, we seek to solve $5\lambda \equiv \alpha \pmod{10}$. $\gcd(5, 10) = 5$ so we must have $5 | \alpha$ meaning that $\alpha = 5$ or 10 . Examining powers of $g = 2$, which are

2	2 ²	2 ³	2 ⁴	2 ⁵	2 ⁶	2 ⁷	2 ⁸	2 ⁹	2 ¹⁰
2	4	8	5	10	9	7	3	6	1

and our theory suggests that only $x^5 \equiv 10 \pmod{11}$ and $x^5 \equiv 1 \pmod{11}$ can be solved while all other $x^5 \equiv a \pmod{11}$ can not be solved.

Checking this,

x	1	2	3	4	5	6	7	8	9	10
x^5	1	10	1	1	1	10	10	10	1	10

3.3 Quadratic residues

Let p be an odd prime. How many of $1 \leq a \leq p-1$ are quadratic residues? We have seen that $\gcd(2, p-1) = 2$ which implies there are $\frac{p-1}{2}$ quadratic residues. We also saw that these quadratic residues come in pairs. $x, p-x$.

For $p = 11$, all quadratic residues appear once as an x^2 with $1 \leq x \leq \frac{p-1}{2}$.

Proposition 3.9. 1. The product of 2 quadratic residues mod p is a quadratic residue,

2. The product of two quadratic non-residues mod p is a quadratic residue, and

3. The product of a quadratic non-residue with a quadratic residue is a quadratic non-residue mod p .

Proof. Write everything in terms of a primitive root, Let $a = g^\alpha, b = g^\beta$ so that $a \cdot b = g^{\alpha+\beta}$ and this result becomes equivalent to parity of the sum of two integers. $\square$

Definition 3.10 (Legendre Symbol). Let p be prime and $a \in \mathbb{Z}$. Define the *Legendre Symbol* as

$$\left(\frac{a}{p}\right) = (a|p) = \begin{cases} +1, & \text{if } a \text{ is a quadratic residue mod } p \\ -1, & \text{if } a \text{ is a quadratic non-residue mod } p \\ 0, & \text{if } a \equiv 0 \pmod{p} \end{cases}$$

Example 3.11. Let $p = 5$, then

a	0	1	2	3	4
$\left(\frac{a}{5}\right)$	0	1	-1	-1	1

If we write $a = g^\alpha$ where g is a primitive root mod p , then a is a quadratic residue if and only if α is even. So (for $a \not\equiv 0 \pmod{p}$) we have

$$\left(\frac{a}{p}\right) = (-1)^\alpha.$$

The above proposition then boils down to say, when $a \equiv g^\alpha, b \equiv g^\beta$,

$$\left(\frac{a \cdot b}{p}\right) = (-1)^{\alpha+\beta} = (-1)^\alpha \cdot (-1)^\beta = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

and this identity extends even when one of a or b is $0 \pmod{p}$.

Question: When is -1 a quadratic residue modulo p ? That is to ask, for which p does $x^2 \equiv -1 \pmod{p}$ have solutions?

Answer: Assuming p is odd then there are solutions if and only if $p = 4k+1$ for some $k \in \mathbb{Z}$. This proof makes use of *Euler's criterion* which we must first discuss.

Lemma 3.12 (Euler's criterion).

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Before this is proven, we remark that the beauty of this formula is that it does not require primitive roots, however it is practically limited.

Proof. First observe that $p-1$ is even (since p is odd). Now, if $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1 \pmod{p}$ (Fermat's Little Theorem). That is, $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$ (this only holds because $p-1$ is even). Hence we must have that $p \nmid a^{\frac{p-1}{2}} \pm 1$ so to say $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Now, either a is a quadratic residue, or it is not. If it is, then $a = g^\alpha$ for some even α , say $\alpha = 2\alpha_0$ so that $a^{\frac{p-1}{2}} \equiv g^{\alpha_0(p-1)} \equiv 1^{\alpha_0} \equiv 1 \pmod{p}$. Hence, in this case $\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Otherwise, then $a = g^\alpha$ with α odd, say $\alpha = 2\alpha_0 + 1$. So, $a^{\frac{p-1}{2}} \equiv g^{\alpha_0(p-1)} \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ (from above). However $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ since g has order $p-1$. Therefore, $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. $\square$

Note that if $a \equiv a' \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.

Question: Suppose a is fixed and we vary p . How does the Legendre symbol depend on p ?

Partial answer: $\left(\frac{a}{p}\right)$ is determined according to $p \pmod{4a}$. We will see that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{iff } p = 4k + 1 \\ -1 & \text{iff } p = 4k + 3 \end{cases}$$

Also,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p = 8k + 1 \text{ or } 8k + 7 \\ -1, & \text{if } p = 8k + 3 \text{ or } 8k + 5 \end{cases}$$

For example, $\left(\frac{2}{11}\right) = -1$ and $11 = 8(1) + 3$.

The first formula here is a simple extension of Euler's formula; $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

A method to the madness of quadratic residues,

Lemma 3.13 (Gauss' Lemma). *Let $a \not\equiv 0 \pmod{p}$. Consider $a, 2a, 3a, \dots, \left(\frac{p-1}{2}\right)a$ with p an odd prime. Reduce them all modulo p so they lie in the interval $(0, p)$. Some will be big (i.e. $> p/2$) and some will be small (i.e. $< p/2$). For the big ones, subtract another multiple of p , so that $ia \equiv r_i \pmod{p}$ with each $-p/2 < r_i < p/2$ for all i .*

For example, if $p = 11$ and $a = 3$ we consider $3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3, 5 \cdot 3 = 3, 6, 9, 1, 4 = 3, -5, -2, 1, 4$.

Let ν represent the number of negative r_i 's resulting from this procedure (so in our example $\nu = 2$). Then, Gauss' Lemma states that

$$\left(\frac{a}{p}\right) = (-1)^\nu.$$

Observe that the r_i 's are just the numbers $1, 2, \dots, \frac{p-1}{2}$, but with each having a signature. So

$$(1 \cdot 3)(2 \cdot 3)(3 \cdot 3)(4 \cdot 3)(5 \cdot 3) \equiv (-1)^2(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5) \pmod{11}$$

which is equivalent to

$$3^5 \equiv (-1)^2 \pmod{11}$$

Now Euler's formula is

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$$

so,

$$\left(\frac{3}{11}\right) = 3^5 \equiv (-1)^2 \equiv 1 \pmod{11}.$$

Let $i \cdot a \equiv r_i \pmod{p}$ with $-p/2 < r_i < p/2$ for each $i = 1, \dots, \frac{p-1}{2}$. We claim that $|r_1|, |r_2|, \dots, |r_{\frac{p-1}{2}}|$ are the numbers $1, 2, 3, \dots, \frac{p-1}{2}$ in some weird order. If the claim is true then

$$\prod_{i=1}^{\frac{p-1}{2}} i \cdot a \equiv (-1)^\nu \prod_{i=1}^{\frac{p-1}{2}} i \pmod{p}$$

Now, since $\gcd(r_i, p) = 1$ for each i , we may cancel the r_i 's on either side, so this is equivalent to

$$a^{\frac{p-1}{2}} \equiv (-1)^\nu \pmod{p}.$$

That is $\left(\frac{a}{p}\right) = (-1)^\nu$. So it remains to prove that $r_i \neq \pm r_j$ for $1 \leq i < j \leq \frac{p-1}{2}$. By construction we have $-p/2 < r_i < p/2$ which implies also that $-\frac{p-1}{2} \leq r_i \leq \frac{p-1}{2}$ and since $r_i \not\equiv 0 \pmod{p}$ because $a \cdot i \not\equiv 0 \pmod{p}$.

We now have two cases;

1. $a \cdot i \equiv a \cdot j \pmod{p}$ means that $p|a(i-j)$ so $p|i-j$ and hence $i \equiv j \pmod{p}$ and finally then $i = j$.
2. $r_i \equiv -r_j \pmod{p}$ implies $p|i+j$, but $3 \leq i+j \leq \frac{p-1}{2} + \frac{p-1}{2} < p$ so $i = j$.

3.4 Applications of Gauss' Lemma

Suppose $a = -1$, then $a, 2a, \dots, \frac{p-1}{2}a$ is $-1, -2, -3, \dots, (-1)\frac{p-1}{2}$. Notice that they already fall in our interval $(-p/2, p/2)$ so there is no need to further reduce. They are also all negative so $\nu = \frac{p-1}{2}$. Hence,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, p = 4k + 1 \\ -1, p = 4k + 3 \end{cases}$$

As a second application, suppose $a = 2$ and p is an odd prime. Then $2, 2 \cdot 2, 3 \cdot 2, \dots, \frac{p-1}{2} \cdot 2 = p-1$. All of these lie in the interval $(0, p)$ so roughly $1/2$ of them are too big. Let us be more specific,

We must now count the even number $2x$ for which $p/2 < 2x < p$. That is how many integers x satisfy $p/4 < x < p/2$? This depends on p modulo 8. Suppose $p = 8k + r$ where

$r = 1, 3, 5$ or 7 . Now $p/4 < x < p/2 \Leftrightarrow 2k + r/4 < x < 4k + r/2$. We are really only concerned with the parity of ν which is equivalent to the number of integers x satisfying $r/4 < x < r/2$;

When $r = 1$ there are no integers in the interval $(1/4, 1/2)$ so ν is even.

When $r = 3$ there is one integer in the interval $(3/4, 3/2)$ so ν is odd.

When $r = 5$ there is one integer in the interval $(5/4, 5/2)$.

When $r = 7$ there are two integers in $(7/4, 7/2)$.

Therefore,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p = 8k + 1 \text{ or } 8k + 7 \\ -1, & \text{if } p = 8k + 3 \text{ or } 8k + 5 \end{cases}$$

3.5 Quadratic reciprocity

Theorem 3.14 (Quadratic Reciprocity). *Let p, q be distinct odd primes, then*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} -1, & \text{if both } p \equiv q \equiv 3 \pmod{4} \\ 1, & \text{else} \end{cases}$$

Euler conjectured while Gauss proved at the age of nineteen that if a is a positive integer and p is an odd prime with $a \not\equiv 0 \pmod{p}$, then the value of $\left(\frac{a}{p}\right)$ is determined by the value of p modulo $4a$. Namely, if $p_1 \equiv p_2 \pmod{4a}$ then $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right)$. Furthermore, by symmetry, if $p_1 \equiv -p_2 \pmod{4a}$ then $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right)$.

Proof. Consider $a, 2a, 3a, \dots, \frac{p-1}{2}a$ and reduce by subtracting multiples of p so they all lie in the interval $[-\frac{p-1}{2}, \frac{p-1}{2}]$. Each of the $i \cdot a$ lie in some interval $(0, p/2), (p/2, p), (p, 3p/2), \dots, ((b-1/2)p, bp)$ and we only need a finite number of these intervals because $b = a/2$ when a is even covers them all and $b = \frac{a-1}{2}$ does when a is odd. We are not omitting any $i \cdot a$ by taking open intervals since none of them are multiples of p or $p/2$. Let $i \cdot a \equiv r_i \pmod{p}$ with each $r_i \in [-\frac{p-1}{2}, \frac{p-1}{2}]$. The negative r_i 's come from multiples which lie in intervals of the form $((b-1/2)p, bp)$ and Gauss' Lemma implies that $\left(\frac{a}{p}\right) = (-1)^\nu$. So how many ax satisfy that $ax \in ((b-1/2)p, bp)$ is equivalent to asking how many integers lie between $(p/2a, p/a), (3p/2a, 2p/a), \dots, ((b-1/2)p/a, bp/a)$, but $p \equiv r \pmod{4a}$ implies $p = 4ak + r$ with $0 \leq r < 4a$ and the intervals become

$$\left(2k + \frac{r}{2a}, 4k + \frac{r}{a}\right), \left(6k + \frac{3r}{2a}, 8k + \frac{2r}{a}\right), \dots, \left((2b-1)2k + \frac{(2b-1)r}{2a}, 4bk + \frac{br}{a}\right).$$

Since we are only interested in the parity of the number of integers between, we may reduce the problem to the intervals $(\frac{r}{2a}, \frac{r}{a}), (\frac{3r}{2a}, \frac{3r}{a}), \dots, (\frac{(2b-1)r}{2a}, \frac{br}{a})$. Now the only dependence of whether ν is even or odd is on r and a . Hence $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right)$ if $p_1 \equiv \pm p_2 \pmod{4a}$. $\square$

Now we are in position to prove Quadratic reciprocity;

Proof. If p, q are distinct odd primes, then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{if at least one of } p, q \text{ are congruent to } 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & \text{if both } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

Verifying this, if $p \equiv q \pmod{4}$ then $4|p - q$ so $p = 4k + q$ for some integer k . Now,

$$\left(\frac{p}{q}\right) = \left(\frac{4k + q}{q}\right) = \left(\frac{4}{q}\right) \left(\frac{k}{q}\right) = \left(\frac{k}{q}\right)$$

and

$$\left(\frac{q}{p}\right) = \left(\frac{p - 4k}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{k}{p}\right) = \begin{cases} -\left(\frac{k}{p}\right), & p \equiv 3 \pmod{4} \\ \left(\frac{k}{p}\right), & p \equiv 1 \pmod{4} \end{cases}$$

So Euler's conjecture implies that $\left(\frac{k}{p}\right) = \left(\frac{k}{q}\right)$ when $p \equiv q \pmod{4}$ so our result holds when $p \equiv q$.

Now, if $p \not\equiv q \pmod{4}$ then $p \equiv -q \pmod{4}$ (i.e. $p \equiv 1$ and $q \equiv 3 \pmod{4}$ or vice versa). So $p \equiv -q \pmod{4}$ meaning that $4|p + q$ and so $p = 4k - q$. Thus,

$$\left(\frac{p}{q}\right) = \left(\frac{4k - q}{q}\right) = \left(\frac{k}{q}\right) = \left(\frac{k}{p}\right) = \dots = \left(\frac{q}{p}\right)$$

and we are done. □

With this, we can compute several Legendre symbols;

Example 3.15.

$$\left(\frac{51}{101}\right) = \left(\frac{3}{101}\right) \left(\frac{17}{101}\right) = \left(\frac{101}{3}\right) \left(\frac{101}{17}\right) = \left(\frac{2}{3}\right) \left(\frac{-1}{17}\right) = (-1)(1) = -1$$

4 Continued fractions

A real number $\alpha \in \mathbb{R}$ may be expressed as $\alpha = q_0 + \alpha'$ where $q_0 \in \mathbb{Z}$ and $\alpha' \in (0, 1)$. Next write $\alpha' = \frac{1}{\alpha_1}$ where $\alpha_1 > 1$. Repeating this process on α provides a way of writing α as a fraction (possibly continuing forever).

Example 4.1.

$$\begin{aligned} \pi &= 3.1415926535\dots = 3 + .1415926\dots \\ &= 3 + \frac{1}{7.06251\dots} \\ &= 3 + \frac{1}{7 + \frac{1}{15.9965\dots}} \\ &= 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{292 + \frac{1}{1 + \dots}}}} \end{aligned}$$

and

$$\frac{93}{37} = 2 + \frac{19}{37} = 2 + \frac{1}{37/19} = 2 + \frac{1}{1 + \frac{18}{19}} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{18}}}$$

Let $A, B \in \mathbb{Z}$ with $B > 0$. Euclidean algorithm gives $A = Bq_0 + r_0, 0 \leq r_0 < B$, $B = q_1r_0 + r_1, 0 \leq r_1 < r_0, \dots, r_{n-2} = q_nr_{n-1} + 0$. So,

$$\frac{A}{B} = q_0 + \frac{r_0}{B} = q_0 + \frac{1}{B/r_0} = q_0 + \frac{1}{q_1 + \frac{r_1}{r_0}} = \dots = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_n}}}}$$

We have shown how to obtain the continued fraction when α is rational and recognized that the continued fraction for a rational number terminates after finitely many steps. Furthermore, the converse of this is true because continued fractions which terminate can be put over a common denominator.

4.1 Finite continued fractions

Consider a fraction of the form

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_n}}}}$$

Are there any patterns?

$$\begin{aligned} q_0 + \frac{1}{q_1} &= \frac{q_0q_1 + 1}{q_1}, \\ q_0 + \frac{1}{q_1 + \frac{1}{q_2}} &= q_0 + \frac{1}{\frac{q_1q_2 + 1}{q_2}} = \frac{q_0q_1q_2 + q_0 + q_2}{q_1q_2 + 1}, \\ q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3}}} &= q_0 + \frac{q_2q_3 + 1}{q_1q_2q_3 + q_1 + q_3} = \frac{q_0q_1q_2q_3 + q_0q_1 + q_3 + q_2q_3 + 1}{q_1q_2q_3 + q_1 + q_3} \end{aligned}$$

This gives a recursion for the numerator and denominator of a continued fraction. Let $[q_0, q_1, q_2, \dots, q_n]$ denote the numerator of the fraction so the denominator will be given by $[q_1, q_2, \dots, q_n]$. The recursion for the numerator is thus,

$$[q_0, q_1, \dots, q_n] = q_0[q_1, \dots, q_n] + [q_2, \dots, q_n].$$

Note that continued fraction for α terminates if and only if α is rational.

Example 4.2.

$$\begin{aligned} [q_0, q_1, q_2, q_3] &= q_0[q_1, q_2, q_3] + [q_2, q_3] \\ &= q_0(q_1[q_2, q_3] + [q_3]) + q_2q_3 + 1 \\ &= q_0(q_1(q_2q_3 + 1) + q_3) + q_2q_3 + 1 \\ &= q_0q_1q_2q_3 + q_0q_1 + q_0q_3 + q_2q_3 + 1 \end{aligned}$$

so now we may write

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_n}}}} = \frac{[q_0, q_1, q_2, \dots, q_n]}{[q_1, q_2, \dots, q_n]}$$

Euler's Rule for continued fractions is that $[q_0, q_1, \dots, q_n]$ is given as the sum of products of q 's where pairs of adjacent q 's are omitted.

Observe

$$[q_0, q_1, q_2, q_3, q_4] = q_0 q_1 q_2 q_3 q_4 + \underbrace{q_2 q_3 q_4 + q_0 q_3 q_4 + q_0 q_1 q_4 + q_0 q_1 q_2}_{\text{omit one adjacent pair}} + \underbrace{q_0 + q_4 + q_2}_{\text{omit two pairs of adjacents}}$$

$$\text{and } [q_0, q_1, q_2, q_3] = q_0 q_1 q_2 q_3 + q_0 q_1 + q_0 q_3 + q_2 q_3 + 1.$$

This is simply proven by induction since we have the recursive formula

$$[q_0, q_1, \dots, q_n] = q_0 [q_1, \dots, q_n] + [q_2, \dots, q_n]$$

Corollary 4.3.

$$[q_0, q_1, \dots, q_n] = [q_n, \dots, q_1, q_0]$$

so that the fractions $q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_n}}}}$ and $q_n + \frac{1}{q_{n-1} + \frac{1}{q_{n-2} + \frac{1}{\dots + \frac{1}{q_0}}}}$ have the same numerator.

For example, $3 + \frac{1}{4 + \frac{1}{5}} = 3 + \frac{5}{21} = \frac{68}{21}$ and $5 + \frac{1}{4 + \frac{1}{3}} = 5 + \frac{3}{13} = \frac{68}{13}$ have the same numerator!

An application of the result is that we may now turn a backwards recursion into a forewords recursion. That is,

$$[q_0, q_1, \dots, q_n] = [q_n, \dots, q_1, q_0] = q_n [q_{n-1}, \dots, q_0] + [q_{n-2}, \dots, q_0]$$

hence if $A_n = [q_0, \dots, q_n]$ then $A_n = q_n A_{n-1} + A_{n-2}$ for $n \geq 2$. Also the denominator is given by $B_n = [q_1, \dots, q_n] = q_n B_{n-1} + B_{n-2}$ for $n \geq 2$. We may also set $A_{-1} = 1, A_{-2} = 0$ so this recursion holds for all n . The advantage now is that extending a continued fraction by one extra partial quotient no longer requires redoing the entire thing from the bottom!

Let $\alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_n}}}}$. The m^{th} partial quotient ($m \leq n$) for α is given by

$$\frac{A_m}{B_m} = \frac{[q_0, q_1, \dots, q_m]}{[q_1, \dots, q_m]}.$$

Example 4.4. Find the continued fraction for $\frac{4321}{123}$ and find all of its partial quotients (i.e. it's convergence).

First, the Euclidean algorithm gives

$$\begin{aligned} 4321 &= 35 \cdot 123 + 16 \\ 123 &= 7 \cdot 16 + 11 \\ 16 &= 1 \cdot 11 + 5 \\ 11 &= 2 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}$$

so

$$\frac{4321}{123} = 35 + \frac{16}{123} = 35 + \frac{1}{7 + \frac{11}{16}} = \cdots = 35 + \frac{1}{7 + \frac{1}{1 + \frac{1}{2 + \frac{1}{5}}}}.$$

Now, the sort way to find the partial quotients is via the following table;

n	q_n	$A_n = q_n A_{n-1} + A_{n-2}$	$B_n = q_n B_{n-1} + B_{n-2}$	$\frac{A_n}{B_n}$
-2	-	0	1	-
-1	-	1	0	-
0	35	35	1	35
1	7	246	7	246/7
2	1	$1(246) + 35 = 281$	8	281/8
3	2	$2(281) + 246 = 808$	$2(8) + 7 = 23$	808/23
4	5	$5(808) + 281 = 4321$	$5(23) + 8 = 123$	4321/123

Lemma 4.5.

$$\frac{A_m}{B_m} - \frac{A_{m-1}}{B_{m-1}} = \frac{B_{m-1}A_m + A_{m-1}B_m}{B_m B_{m-1}} = \frac{(-1)^m}{B_m B_{m-1}}$$

That is, they alternate in sign.

Proof. By induction, when $m = -1$ we have $A_{-1}B_{-2} - A_{-2}B_{-1} = 1 \cdot 1 - 0 \cdot 0 = (-1)^2$ which is good. Assuming now that the result holds for $m - 1$ and considering the m^{th} case ($m \geq 0$), then

$$\begin{aligned} A_m B_{m-1} A_{m-1} B_m &= (q_m A_{m-1} + A_{m-2}) B_{m-1} - A_{m-1} (q_m B_{m-1} + B_{m-2}) \\ &= A_{m-2} B_{m-1} - A_{m-1} B_{m-2} \\ &= -(A_{m-1} B_{m-2} - A_{m-2} B_{m-1}) = (-1)^{m-1}. \end{aligned}$$

□

Corollary 4.6. $\frac{A_m}{B_m}$ is in reduced form. That is $\gcd(A_m, B_m) = 1$.

Proof. Let $\gcd(A_m, B_m) = d \geq 1$ and we have $A_m B_{m-1} - A_{m-1} B_m = (-1)^{m-1}$. Since $d|A_m$ and $d|B_m$ then $d|A_m B_{m-1} - A_{m-1} B_m = (-1)^{m-1}$ implying $d = 1$. □

4.2 Infinite continued fractions

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ (i.e. α is irrational). The procedure $\alpha = q_0 + \frac{1}{\alpha_1}$ with $q_0 \in \mathbb{Z}$ and $\alpha_1 > 1$ can be repeated on α_1 and yields a continued fraction for α . After $n + 1$ repetitions of this, one will have

$$\alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_n + \frac{1}{\alpha_{n+1}}}}}}$$

and never terminates. That is to say $\alpha_{n+1} \neq 0$ since α is irrational. Note that for rationals $\alpha_{n+1} = \infty$. So in this case we write $\alpha = \frac{[q_0, q_1, \dots, q_n, \alpha_{n+1}]}{[q_1, q_2, \dots, q_n, \alpha_{n+1}]}$ where

$$[q_0, q_1, \dots, q_n, \alpha_{n+1}] = \alpha_{n+1} A_n + A_{n-1} \text{ and } [q_1, \dots, q_n, \alpha_{n+1}] = \alpha_{n+1} B_n + B_{n-1}$$

and so we could also write

$$\alpha = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}.$$

Question: How well do convergents $\frac{A_i}{B_i}$ approximate α ? Equivalently, how small is $\left|\alpha - \frac{A_n}{B_n}\right|$?

Theorem 4.7. $\left|\alpha - \frac{A_n}{B_n}\right| < \frac{1}{B_n B_{n+1}}$ for all $n \geq 0$. Furthermore, this implies $\left|\alpha - \frac{A_n}{B_n}\right| \rightarrow 0$ as $n \rightarrow \infty$ because B_n is a monotonically increasing sequence of integers ($B_n = q_n B_{n-1} + B_{n-2} > B_{n-1}$).

Proof. Consider the difference

$$\begin{aligned} \alpha - \frac{A_n}{B_n} &= \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} - \frac{A_n}{B_n} \\ &= \frac{\alpha_{n+1}B_n A_n + A_{n-1}B_n - \alpha_{n+1}A_n B_n - A_n B_{n-1}}{B_n(\alpha_{n+1}B_n + B_{n-1})} \\ &= \frac{(-1)^n}{B_n(\alpha_{n+1}B_n + B_{n-1})} \\ &< \frac{(-1)^n}{B_n(q_{n+1}B_n + B_{n-1})} \\ &= \frac{(-1)^n}{B_n B_{n+1}} \end{aligned}$$

where the inequality holds because $\alpha_{n+1} = q_{n+1} + \frac{1}{\alpha_{n+2}} > q_{n+1}$ and this yields the desired result. $\square$

Another important observation to make is that the sequence given by $\left|\alpha - \frac{A_n}{B_n}\right|$ is monotonically decreasing. Continued fractions provide best approximations of irrational numbers in the sense that if $\frac{A_n}{B_n}$ is the n^{th} convergent to α , then any other $\frac{a}{b} \in \mathbb{Q}$ which is closer to α must have $b > B_n$ (i.e. larger denominator).

An application of this answers the question “Why are there 12 notes to an octave?” There are 3 constraints here.

1. Desire to modulate (i.e. transpose ratio between successive is constant, say r),
2. Must capture an octave,
3. Want to capture a perfect 5^{th} .

This means³ we want $r^a = \frac{3}{2}$ for some $a \in \mathbb{Z}$. This implies⁴ $2^{a/k} = 3/2$ which can't be done because this is $2^a = (3/2)^k$ so $2^{a+k} = 3^k$ and violates prime factorization. We should thus find ratios a/k such that $2^{a/k} \approx 3/2$. Examine $2^x = 3/2$ whose solution is $x = \log_2(3/2) = 0.5849625\dots$ and is irrational. Finding rational numbers close to x using continued fractions (since they give the best approximations). We find that $x = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{3 + \dots}}}}}$

and convergents are $0, 1, 1/2, 3/5, 7/12, 24/41$ which suggests a 12 note octave with a perfect

³I do not understand any of this

⁴why?

3. A quadratic irrational is called *reduced* if $\alpha > 1$ and its conjugate satisfies $-1 < \alpha' < 0$.

Theorem 4.11. α has a purely periodic continued fraction if and only if α is reduced.

Proof. Suppose first that α has a purely periodic continued fraction so that $\alpha = q_0 + \frac{1}{q_1 + \frac{1}{\ddots + \frac{1}{q_n + \frac{1}{\alpha}}}}$ which give a quadratic irrational (we know it irrational since the continued fraction doesn't terminate). Consider β obtained by reversing the period of α . That is,

$$\beta = q_n + \frac{1}{q_{n-1} + \frac{1}{\ddots + \frac{1}{q_0 + \frac{1}{\beta}}}} = \frac{[q_n, \dots, q_0, \beta]}{[q_{n-1}, \dots, q_0, \beta]} = \frac{\beta[q_n, \dots, q_0] + [q_n, \dots, q_1]}{\beta[q_{n-1}, \dots, q_0] + [q_{n-1}, \dots, q_1]} = \frac{\beta A_n + B_n}{\beta A_{n-1} + B_{n-1}}.$$

So, α, β satisfy $\alpha = \frac{\alpha A_n + A_{n-1}}{\alpha B_n + B_{n-1}}, \beta = \frac{\beta A_n + B_n}{\beta A_{n-1} + B_{n-1}}$ which are equivalent to

$$B_n \alpha^2 + (B_{n-1} - A_n) \alpha - A_{n-1} = 0$$

and

$$A_{n-1} \beta^2 + (B_{n-1} - A_n) \beta - B_n = 0$$

multiplying the second equation by $\frac{-1}{\beta^2}$ then becomes

$$B_n \left(\frac{-1}{\beta^2} \right) + (B_{n-1} - A_n) \left(\frac{-1}{\beta^2} \right) - B_n = 0$$

meaning that α and $-1/\beta$ are conjugates (i.e. distinct roots of the same quadratic equation). Now, $\beta = q_n + \frac{1}{\dots} > q_n \geq 1$ implies $-1 < -1/\beta < 0$ so α is reduced.

Conversely, suppose α is reduced so that it is a quadratic irrational with $\alpha > 1$ and $\alpha' \in (-1, 0)$. More precisely this means $a\alpha^2 + b\alpha + c = 0$ for some $a, b, c \in \mathbb{Z}$ so that $\alpha = \frac{-b + \sqrt{b^2 - 4ac}}{2a} = \frac{P + \sqrt{D}}{Q}$. So $D = b^2 - 4ac$ is square free and positive, $P = -b$ and $Q = 2a$ while $\alpha' = \frac{P - \sqrt{D}}{Q}$.

Lemma 4.12. α reduced implies

- (i) Both $P, Q > 0$,
- (ii) $Q \mid P^2 - D$, and
- (iii) $P < \sqrt{D}, Q < 2\sqrt{D}$.

proof: For (ii), observe $P^2 - D = b^2 - b^2 + 4ac = 4ac = 2a \cdot 2c$ and $Q = 2a$. For (i) $Q > 0$ by assumption and $\alpha > 1, \alpha' > -1$ means $\alpha + \alpha' > 0$ which means $\frac{2P}{Q} > 0$ so $P > 0$ since $Q > 0$. Finally, for (iii) $\alpha > 1$ so $\frac{P + \sqrt{D}}{Q} > 1$ which implies $Q < P + \sqrt{D} < 2\sqrt{D}$ since $P < \sqrt{D}$ because $\alpha' = \frac{P - \sqrt{D}}{Q} < 0$ meaning $P < \sqrt{D}$.

As second lemma states;

Lemma 4.13. Consider the continued fraction from the algorithm $\alpha = q_0 + \frac{1}{\alpha_1}$ where q_0 is the integer part of α . If α is reduced then so is α_1 . Furthermore, α_1 takes the form $\alpha_1 = \frac{P_1 + \sqrt{D}}{Q_1}$ for the same D as α and $P_1, Q_1 \in \mathbb{Z}$.

proof: Let $\alpha = q_0 + \frac{1}{\alpha_1}$ so that $\alpha_1 = \alpha - q_0 = \frac{P+\sqrt{D}}{Q} - q_0 = \frac{(P-Qq_0)+\sqrt{D}}{Q}$. Declare that $-P_1 = P - Qq_0$ so to say $\alpha_1 = \frac{Q}{-P_1+\sqrt{D}}$. Simplifying this gives

$$\alpha_1 = \frac{Q}{P_1^2 - D} \cdot (-P_1 - \sqrt{D}) = \frac{P_1 + \sqrt{D}}{\frac{D-P_1^2}{Q}} = \frac{P_1 + \sqrt{D}}{Q_1}$$

since $D - P_1^2 = D - P^2 - 2PQq_0 + Q^2q_0$ so $Q|D - P_1^2$ and $Q_1 \in \mathbb{Z}$.

Apparently this is the end of the proof. $\square$

An application of this is to provide a continued fraction for $\sqrt{N} \in \mathbb{N} \setminus \{\text{perfect squares}\}$.

Claim: $\sqrt{N} + q_0$ where $q_0 = \lfloor \sqrt{N} \rfloor$ is purely periodic.

Proof. 1. $\sqrt{N} + q_0$ is a quadratic irrational since $\alpha = \sqrt{N} + q_0$ which implies $(\alpha - q_0)^2 = N$ so that $\alpha^2 - 2q_0\alpha + q_0^2 - N = 0$.

2. $\sqrt{N} + q_0 > 1$

3. $q_0 - \sqrt{N} \in (0, 1)$ since $q_0 = \lfloor \sqrt{N} \rfloor$ which implies $\sqrt{N} \in (q_0, q_0 + 1)$ and $-\sqrt{N} \in (-q_0 - 1, -q_0)$ so that $-\sqrt{N} + q_0 \in (-1, 0)$. $\square$

4.3 Pell's equations

These come up when trying to find units in real quadratic fields. Let N be a positive integer which is not a square. Pell's equation is

$$x^2 - Ny^2 = 1.$$

and we wish to find positive integer solutions $x, y \in \mathbb{Z}$ to the equation $1 = (x - \sqrt{N}y)(x + \sqrt{N}y)$. This implies

$$\left(\frac{x}{y} - \sqrt{N}\right) = \frac{1}{y(x + \sqrt{N}y)} < \frac{1}{y(\sqrt{N}y + \sqrt{N}y)} = \frac{1}{2y^2\sqrt{N}}$$

where the inequality holds since $x^2 = Ny^2 + 1 > Ny^2$ so $x > \sqrt{N}y$.

So a pair of integer solutions to $x^2 - Ny^2 = 1$ give an approximation to $\sqrt{N}$. Namely $\left|\frac{x}{y} - \sqrt{N}\right| < \frac{1}{2y^2\sqrt{N}}$ which beats the typical convergent to $\sqrt{N}$ by quite a bit. We learned that continued fractions give best approximations to reals. This suggests looking at the continued fraction for $\sqrt{N}$, but only certain types of convergence will give this tight of an approximation.

Consider $\frac{A_n}{B_n}, \frac{A_{n-1}}{B_{n-1}}$ (the two convergence that appear before the $2q_0$ term)

$$\begin{aligned} \sqrt{N} &= q_0, \overline{q_1, q_2, \dots, q_n, 2q_0} \\ &= \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}, \quad \alpha_{n+1} = 2q_0 + \frac{1}{q_1 + \frac{1}{\ddots + \frac{1}{q_n + \frac{1}{2q_0 + \frac{1}{\ddots}}}}} \\ &= \frac{(\sqrt{N} + q_0)A_n + A_{n-1}}{(\sqrt{N} + q_0)B_n + B_{n-1}} \end{aligned}$$

This implies $NB_n + (q_0B_n + B_{n-1})\sqrt{N} = q_0A_n + A_{n-1} + A_n\sqrt{N}$ and comparing coefficients gives $NB_n = q_0A_n + A_{n-1}$ and $A_n = q_0B_n + B_{n-1}$ meaning $A_{n-1} = NB_n - q_0A_n$ and $B_{n-1} = A_n - q_0B_n$. Now, $A_nB_{n-1} - B_nA_{n-1} = (-1)^{n-1}$ so $A_n(A_n - q_0B_n) - B_n(NB_n - q_0A_n) = (-1)^{n-1}$ and hence

$$A_n^2 - NB_n^2 = (-1)^{n-1}.$$

So when n is odd, this is a solution to Pell's equations. If n is even, we go up by $n + 1$ convergence to $\frac{A_{2n+1}}{B_{2n+1}}, \frac{A_{2n}}{B_{2n}}$ and the proof is the same. In general we get

$$A_{kn+k-1}^2 - NB_{kn+k-1}^2 = (-1)^{kn+k-2}$$

and $kn + k - 2 \equiv k(n + 1) \equiv 0 \pmod{2}$ if and only if n is odd or k is even.

5 Partitions

How many ways can we add up to an integer from a given set? Some classical problems involving this are sums of positive integers, sums of squares, cubes, etc. and the Goldbach conjecture about sums of primes.

An easy problem; how many ways are there to add to $n \in \mathbb{N}$ using positive integers where the order is taken into consideration? Place n dots on the page in a row, there are 2^{n-1} ways to insert a barrier or not between each of these dots. This is equivalent to partitioning n into a sum of positive integers where order counts. Hence $c(n)$, the number of ways to write n as a sum of positive integers, is 2^{n-1} .

If order doesn't count, then $c(n) = [x^n] \prod_{i \geq 1} (1 - x^i)^{-1}$. The following result relates partitions to pentagonal numbers.

Theorem 5.1 (Euler's Pentagonal Number Theorem).

$$\prod_{n=1}^{\infty} (1 - x^n) = \sum_{k=-\infty}^{\infty} (-1)^k x^{\omega(n)} = 1 + \sum_{k=1}^{\infty} (-1)^k (x^{k(3k+1)/2} + x^{k(3k-1)/2})$$

where $\omega(n) = \frac{3n^2 - n}{2} \geq 0$ are called pentagonal numbers.

Hardy and Littlewood show using $\prod_{i \geq 1} (1 - x^i)^{-1} = \sum p(n) x^n$ with $p(n) \approx \frac{e^{\pi(2/3)^{1/2} \sqrt{n}}}{4n\sqrt{3}}$. Ramanujan wrote, with $q = e^{2\pi iz}$ and $\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$ and $\tau(ab) = \tau(a)\tau(b)$ when a, b are coprime. Now, $\Delta(-1/z) = z^{12} \Delta(z)$ is the first example of an integer weight modular form.

Let $r_k(n)$ be the number of ways of writing $n \in \mathbb{Z}$ as a sum of k -squares (allowing negatives and zeros). One finds that $r_2(n) = 4(d_1(n) - d_3(n))$ where $d_k(n)$ is the number of divisors of n congruent to k modulo 4. Note that $r_2(n) \geq 4$ if n does not have a prime of the form $4k + 3$ raised to an odd power in its prime factorization.

Furthermore,

$$r_4(n) = \begin{cases} 8 \sum_{d|n} d, & \text{if } n \geq 8 \text{ is odd} \\ 24 \sum_{d|n, \text{ odd}} d, & \text{if } n \geq 8 \text{ is even} \end{cases}$$

which implies all positive integers m can be expressed as the sum of four squares.

Theorem 5.2 (Euler). *Let $p = 4k + 1$ be prime. Then p can be written as the sum of squares.*

Proof. With $p \equiv 1 \pmod{4}$ the congruence can be solved by $z^2 \equiv -1 \pmod{p}$ for some $1 \leq z < p$.

Now, $p|z^2 + 1$ implies $z^2 + 1 = mp$ for some $m \in \mathbb{Z}$ with $1 \leq m < p$. If mp can be written as the sum of two squares with $1 \leq m < p$ then there exists an r with $1 \leq r < m$ such that $rp = x_1^2 + y_1^2$. Repeat this process until $r = 1$. To demonstrate that this is true, reduce x, y modulo m chosen to lie in the interval $(-m/2, m/2)$. That is $x \equiv u, y \equiv v \pmod{m}$ with both $-m/2 < u, v < m/2$. Now $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ where $u^2 + v^2 = rm$ for some $r \geq 0$. Since $m \geq 1$ and the left hand side is positive, this furthermore means that $r \neq 0$ because otherwise $u = v = 0$, $m|x, m|y$ so $m^2|x^2 + y^2 = mp$ but this implies $m|p$ (a contradiction).

Thus, $u^2 + v^2 = rm$ with $r \geq 1$. Now,

$$r = \frac{u^2 + v^2}{m} \leq \frac{\frac{m^2}{4} + \frac{m^2}{4}}{m} = \frac{m}{2} < m$$

so $r < m$.

$$(mp)(rm) = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2$$

by Fibonacci. Thus, a product of squares is a sum of two squares. $xu + yv \equiv x^2 + y^2 \equiv 0 \pmod{m}$ and $xv - yu \equiv xy - yx \pmod{m}$ meaning that $m^2|(xu + yv)^2$ and $m^2|(xv - yu)^2$ so that $rp = x_1^2 + y_1^2$. $\square$