Background in elementary number theory

Notation: X = set $\quad |X|$ = the number of elements of X

$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$, $\quad \mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}$

$\mathbb{N} = \{0, 1, 2, \dots\} = \mathbb{Z}_{\geq 0}$, $\quad \mathbb{N}_+ = \{1, 2, \dots\} = \mathbb{Z}_{>0}$

Recall: • (for $a, b \in \mathbb{Z}$) b **divides** a (notation: $b \mid a$) if $\exists c \in \mathbb{Z}$ $\quad a = bc$ $\quad (\Leftrightarrow a\mathbb{Z} \subset b\mathbb{Z})$

• a **prime number** is an integer $p > 1$ which is not a product in a nontrivial way: $p \neq ab$ for any integers $1 < a, b < p$.

Notation: $\mathcal{P} = \{$ prime numbers $\} = \{2, 3, 5, 7, 11, \dots\}$

Existence of prime factorisation: every integer $n \geq 1$ can be written as a (possibly empty) product of (not necessarily distinct) primes. [proof: easy induction on n]

Thm: There are infinitely many prime numbers ($|\mathcal{P}| = \infty$).

Pf. Enough to show: for any finite subset $S = \{p_1, \dots, p_r\} \subset \mathcal{P}$ $(r \geq 0)$ there exists $p \in \mathcal{P}$, $p \notin S$. Consider $N := p_1 \cdots p_r + 1 \geq 2$ $(N = 2 \Leftrightarrow r = 0)$. Prime factorisation of N implies that $\exists\ p \in \mathcal{P}$, $p \mid N$. If $p \in S$, then $p \mid \underbrace{p_1 \cdots p_r}_{N-1} \Rightarrow p \mid \underbrace{N - (N-1)}_{1}$ impossible.

So $p \notin S$.

Variant. $|\mathcal{P} \cap \underbrace{(4\mathbb{Z}+3)}_{\{4k+3 \mid k \in \mathbb{Z}\}}| = \infty$

Pf: $\mathcal{P} = \{2\} \cup (\mathcal{P} \cap (4\mathbb{Z}+3)) \cup (\mathcal{P} \cap (4\mathbb{Z}+1))$. Given $S = \{p_1, \dots, p_r\} \subset \mathcal{P} \cap (4\mathbb{Z}+3)$ $(r \geq 0)$, consider $N := 4p_1 \cdots p_r + 1 \geq 3$ $(N = 3 \Leftrightarrow r = 0)$. As $2 \nmid N$, every prime $p \mid N$ lies either in $\mathcal{P} \cap (4\mathbb{Z}+3)$, or in $\mathcal{P} \cap (4\mathbb{Z}+1)$. If all primes $p \mid N$ lie in $4\mathbb{Z}+1$, so does N (since $4\mathbb{Z}+1$ is closed under multiplication), but this is not true. Therefore $\exists\ p \mid N$ such that $p \notin \mathcal{P} \cap (4\mathbb{Z}+1) \Rightarrow \underline{p \in \mathcal{P} \cap (4\mathbb{Z}+3)}$. Again, if $p \in S$, then $p \mid \underbrace{4p_1 \cdots p_r}_{N+1} \Rightarrow p \mid \underbrace{(N+1) - N}_{1}$ impossible.

So $p \notin S$.

Question. Does this argument prove $\underbrace{|\mathcal{P} \cap (m\mathbb{Z}+a)| = \infty}_{\text{true if } \gcd(m,a) = 1 \text{ (Dirichlet's thm)}}$ in other cases?

Prime numbers of special form

Mersenne numbers: $\boxed{M_n = 2^n - 1}$

n	M_n
1	1
(2)	(3)
(3)	(7)
4	$15 = 3 \cdot 5$
(5)	(31)
6	$63 = 3^2 \cdot 7$
(7)	(127)
8	$255 = 3 \cdot 5 \cdot 17$
9	$511 = 7 \cdot 73$
10	$1023 = 3 \cdot 11 \cdot 31$
(11)	$2047 = 23 \cdot 89 \neq$ prime

primes

Facts: (1) M_n is a prime $\Rightarrow$ $n = p$ is a prime

(but not "$\Leftarrow$": $M_{11} \notin P$)

Pf: $M_1 = 1 \notin P$. If $n = ab$ ($a, b > 1$), then $M_n = 2^{ab} - 1 = \underbrace{(2^a - 1)}_{>1}\underbrace{(2^{a(b-1)} + \dots + 2^a + 1)}_{\geq 1}$.

(2) ∃ reasonably effective criterion for deciding whether $M_p \in P$ (even for large primes $p \in P$)

Question: what about $(3^n - 1)/2$?

What about $2^n + 1$?

n	$2^n + 1$
1	(3)
2	(5)
3	$9 = 3^2$
4	(17)
5	$33 = 3 \cdot 11$
6	$65 = 5 \cdot 13$
7	$129 = 3 \cdot 43$
8	(257)

Proposition: $2^n + 1$ is a prime $\Rightarrow$ $n = 2^m$.

Pf: If $n \neq 2^m \Rightarrow n = ab$, $a \geq 1$, $b > 1$, $2 \nmid b$

$2^n + 1 = (2^a)^b + 1 = \underbrace{(2^a + 1)}_{>1}\underbrace{((2^a)^{b-1} - (2^a)^{b-2} + \dots - 2^a + 1)}_{>1}$.

Def. Fermat numbers: $F_m := 2^{(2^m)} + 1$.

m	0	1	2	3	4
F_m	3	5	17	257	65537

prime numbers

Euler: $641 \mid F_5$ ($\Rightarrow F_5 = 2^{32} + 1 \notin P$).

At present (2017), no Fermat number F_m for $m > 4$ is known to be a prime.

Fact: if $d \mid F_m \Rightarrow d \equiv 1 \pmod{2^{m+1}}$.

Uniqueness of prime factorisation

Every integer $n \geq 1$ can be written as a product of prime numbers in a unique way (up to a permutation of factors):

$$n = \pm \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

(the exponent $\underbrace{v_p(n) \in \mathbb{N}_+}$ is equal to zero for all but finitely many p)
(the p-adic valuation of n)

and each $v_p(n)$ is determined by n.

Proof of uniqueness – key steps (details – later in more generality

Uniqueness of prime factorisation $\Leftarrow$ Euclid's Lemma:
$p \in \mathbb{P}$, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

$\Uparrow$

Bézout property of $\mathbb{Z}$:
$\forall a,b \in \mathbb{Z} \quad \exists d \in \mathbb{Z} \quad \underbrace{a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}}$
(d unique up to a sign) $\{ax+by \mid x,y \in \mathbb{Z}\}$

If $a,b \neq 0 \Rightarrow$ can take $d>0$ unique

$d = \gcd(a,b)$
the greatest common divisor of a,b

$\Uparrow$

Euclid's algorithm

$\Uparrow$

Division (with remainder)

$\forall a,b \in \mathbb{Z},\ b \neq 0 \quad \exists q,r \in \mathbb{Z} \quad a = qb + r$
q: quotient, r: remainder, $|r| < |b|$

Consequences : • each $a \in \mathbb{Q} \setminus \{0\}$ is written in a unique way

$$a = \pm \prod_{p \in \mathbb{P}} p^{v_p(a)}, \qquad \underbrace{v_p(a) \in \mathbb{Z}}$$

($=0$ for all but finitely many p)
the p-adic valuation of a

- $v_p(ab) = v_p(a) + v_p(b)$
- $a \in \mathbb{Z} \setminus \{0\} \iff \forall p \in \mathbb{P} \quad v_p(a) \geq 0$
- For $a,b \in \mathbb{Z} \setminus \{0\}$, $b \mid a \iff \forall p \in \mathbb{P} \quad v_p(b) \leq v_p(a)$
- $v_p(a+b) \geq \min(v_p(a), v_p(b))$

• For $a, r \in \mathbb{N}_+$, $\left[\sqrt[r]{a} \in \mathbb{Q} \iff \sqrt[r]{a} \in \mathbb{Z} \left(\iff \exists b \in \mathbb{N}_+ \ a = b^r\right)\right]$

[Pf. of "$\Rightarrow$": if $a = b^r$, $b \in \mathbb{Q}_{>0}$, then $\forall p \in \mathcal{P} \quad 0 \le r \cdot v_p(b) = v_p(a) \Rightarrow b \in \mathbb{Z}$, $b > 0$]

(So $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \ldots \notin \mathbb{Q}$)

• For $a = \pm \prod_p p^{v_p(a)}$, $b = \pm \prod_p p^{v_p(b)} \in \mathbb{Z} \setminus \{0\}$, the integers (positive)

$d := \prod_p p^{\min(v_p(a), v_p(b))}$, $e := \prod_p p^{\max(v_p(a), v_p(b))} \in \mathbb{N}_+$ satisfy

- $d \mid a$, $d \mid b$, [if $c \mid a$ and $c \mid b \Rightarrow c \mid d$]

($d =: \gcd(a,b)$ is the greatest common divisor of a and b)

- $a \mid e$, $b \mid e$, [if $a \mid c$ and $b \mid c \Rightarrow e \mid c$]

($e =: \operatorname{lcm}(a,b)$ is the least common multiple of a and b)

Note: for $a, b \in \mathbb{Z} \setminus \{0\}$, $a\mathbb{Z} + b\mathbb{Z} = d'\mathbb{Z}$ for unique $d' \in \mathbb{N}_+$. this equality implies that $a\mathbb{Z}, b\mathbb{Z} \subset d'\mathbb{Z}$ ($\iff d' \mid a$ and $d' \mid b$), and also that $\gcd(a,b)$ divides each element of $a\mathbb{Z} + b\mathbb{Z}$, so $\gcd(a,b) \mid d'$

$\iff d' \mid \gcd(a,b)$

$$\boxed{a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}} \Leftarrow$$

• If $d = \gcd(a,b)$ $(a, b \in \mathbb{Z} \setminus \{0\})$, then $a = da'$, $b = db'$, $\gcd(a', b') = 1$

• If $a, b, c \in \mathbb{Z} \setminus \{0\}$, $\gcd(c, a) = 1$ and $c \mid ab$, then $c \mid b$

(generalisation of Euclid's lemma)

• If $a, b, c \in \mathbb{Z} \setminus \{0\}$, $r \in \mathbb{N}_+$, $ab = c^r$ and $\gcd(a,b) = 1$, then $\exists\ a_1, b_1 \in \mathbb{Z} \setminus \{0\}$ $a = \pm a_1^r$, $b = \pm b_1^r$

Pf: $\forall p \in \mathcal{P}$ $v_p(a) + v_p(b) = v_p(ab) = r \cdot v_p(c)$ is divisible by r

(at least one of them is 0, since $\gcd(a,b) = 1$)

$\Rightarrow \forall p \in \mathcal{P}$ $v_p(a), v_p(b)$ are divisible by r

Congruences modulo n $(n \ge 1)$

Recall: for $a, b \in \mathbb{Z}$ $a \equiv b \pmod n$ if $n \mid (a-b)$

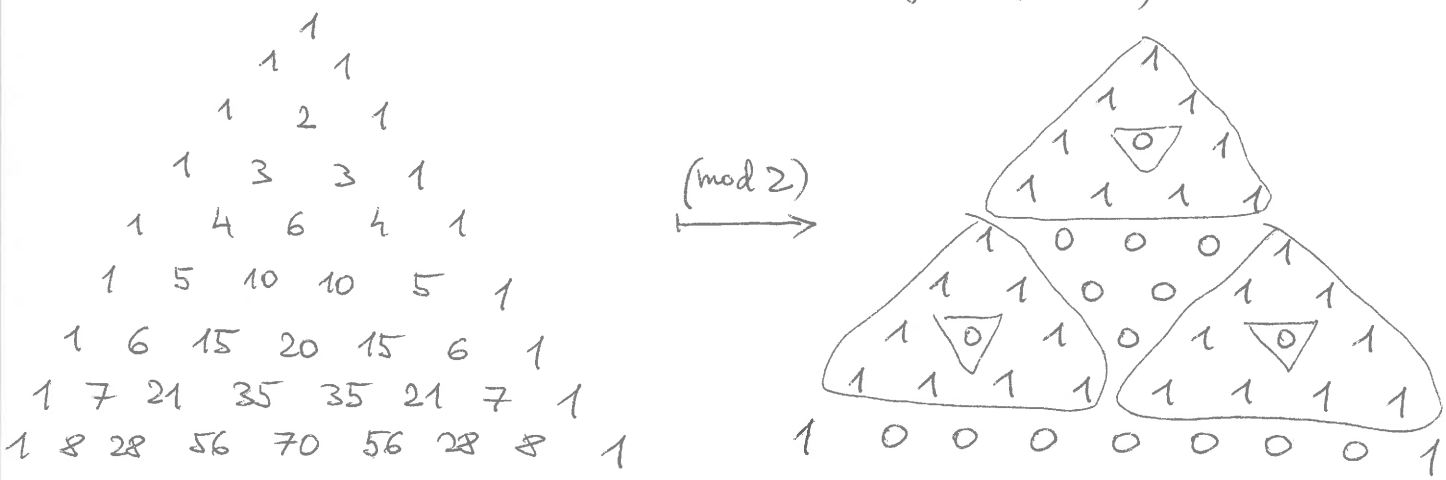
• $\mathbb{Z} = \bigsqcup_{i=0}^{n-1} (a + n\mathbb{Z})$ n disjoint residue classes modulo n

• $\begin{matrix} a \equiv b \\ a' \equiv b' \end{matrix} \pmod n \Rightarrow \begin{matrix} a \pm a' \equiv b \pm b' \\ aa' \equiv bb' \end{matrix} \pmod n$

So $\forall f \in \mathbb{Z}[X]$ $a \equiv b \pmod n \Rightarrow f(a) \equiv f(b) \pmod n$

Binomial coefficients (mod p)

Exercise 1. (a) Consider the "Pascal triangle" (mod 2):



What is going on ? Can you guess the rule ?

(b) Idem for (mod 3). (c) Idem for (mod p) (p = prime).

Exercise 2. Let p be a prime, let $m, n \in \mathbb{N}_+$.

(a) $v_p(n!) = \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor = \frac{n - s_p(n)}{p-1}$, where $n = a_0 + p a_1 + \cdots + p^k a_k$ $(k \geq 0)$,

$a_i \in \{0, 1, \ldots, p-1\}$, $s_p(n) = a_0 + a_1 + \cdots + a_k$. (the digits of n in base p)

(b) $v_p\left(\frac{(pn)!}{n!}\right) = n$. (c) $v_p\left(\binom{pn}{pm}\right) = v_p\left(\binom{n}{m}\right)$.

Exercise 3. Let p be a prime, let $n \in \mathbb{N}_+$.

(a) If $a, b \in \mathbb{N}$, $a', b' \in \{0, 1, \ldots, p-1\} \Rightarrow \binom{pa+a'}{pb+b'} \equiv \binom{a}{b}\binom{a'}{b'} \pmod p$.

(b) — " — , $a_i, b_i \in \{$ — " — $\} \Rightarrow \binom{a_0 + p a_1 + \cdots + p^k a_k + p^{k+1} a}{b_0 + p b_1 + \cdots + p^k b_k + p^{k+1} b} \equiv \binom{a}{b} \prod_{i=1}^{k} \binom{a_i}{b_i} \pmod p$

(c) $\left[\forall m \in \{1, 2, \ldots, n-1\} \quad p \mid \binom{n}{m}\right] \Leftrightarrow \exists k \in \mathbb{N}_+ \quad n = p^k$.

(d) (If $n > 1$) $\left[\forall m \in \{0, 1, \ldots, n\} \quad p \nmid \binom{n}{m}\right] \Leftrightarrow \exists k \in \mathbb{N}_+ \quad n = p^k - 1$.

(e) If $n = a_0 + p a_1 + \cdots + p^k a_k$ $(a_i \in \{0, 1, \ldots, p-1\})$, then

$$\left| \left\{ j \mid 0 \leq j \leq n, \; p \nmid \binom{n}{j} \right\} \right| = \prod_{i=0}^{k} (a_i + 1).$$

(f) Determine, for each $k \geq 1$, $\left| \left\{ (m, n) \;\middle|\; \begin{array}{l} 0 \leq n < p^k, \\ 0 \leq m \leq n \end{array}, \; p \nmid \binom{n}{m} \right\} \right|$.

Exercise 4. What is the relation between Ex. 1 and Ex. 2, 3 ?

Invertible residue classes: let $n \in \mathbb{N}_+$

Prop. For $a \in \mathbb{Z}$, $[\exists a' \in \mathbb{Z}\ \ a'a \equiv 1 \pmod n \iff \gcd(a,n)=1]$

Pf: $1 \in a\mathbb{Z} + n\mathbb{Z} = \gcd(a,n)\mathbb{Z}$

Euler's function: for $n \geq 1$, $\varphi(n) := |\{1 \leq a \leq n \mid \gcd(a,n)=1\}|$

(the number of invertible residue classes $(\bmod n)$).

Properties of $\varphi(n)$: (1) $\varphi(1)=1$.

(2) If $n=p^k$, p prime, $k \geq 1$: for $1 \leq a \leq p^k$, $\gcd(a,p^k) \neq 1 \iff a = pb$, $1 \leq b \leq p^{k-1}$

$\Rightarrow \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1-\frac{1}{p}\right)$.

(3) If $n = p_1^{k_1} \cdots p_r^{k_r}$ $(r \geq 0$, p_i distinct primes, $k_i \geq 1)$: let $A := \{1, 2, \dots, n\}$, $A_\alpha := \{a \in A \mid p_\alpha \text{ divides } a\}$ $(1 \leq \alpha \leq r)$. Then

$\{a \in A \mid \gcd(a,n) \neq 1\} = A_{\alpha_1} \cup \cdots \cup A_{\alpha_r}$

cardinality $= n - \varphi(n)$

cardinality $= \sum_\alpha \underbrace{|A_\alpha|}_{\frac{n}{p_\alpha}} - \sum_{\alpha<\beta} \underbrace{|A_\alpha \cap A_\beta|}_{\frac{n}{p_\alpha p_\beta}} + \sum_{\alpha<\beta<\gamma} |A_\alpha \cap A_\beta \cap A_\gamma| - \cdots$

$\Rightarrow \varphi(n) = n\left(1 - \sum_\alpha \frac{1}{p_\alpha} + \sum_{\alpha<\beta} \frac{1}{p_\alpha p_\beta} - \cdots + (-1)^r \frac{1}{p_1 \cdots p_r}\right) = n \prod_{\alpha=1}^{r} \left(1 - \frac{1}{p_\alpha}\right)$

---

(4) If $\gcd(m,n)=1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

Reformulation: for $1 \leq a \leq n$, the fraction $\frac{a}{n}$ (written in its lowest terms) has denominator $d \iff d \mid n$ and $\gcd(a,n) = n/d$

$\iff a = \frac{n}{d}a'$, $1 \leq a' \leq d$, $(a',d)=1$. Therefore the set of fractions $\{\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ written in the lowest terms$\}$ contains, for each $d \mid n$, precisely $\varphi(d)$ fractions with denominator $\varphi(d)$.

So: $\boxed{\sum_{d \mid n} \varphi(d) = n}$

Ex $(n=6)$ $\frac{1}{6}, \underbrace{\frac{2}{6}}_{\frac{1}{3}}, \underbrace{\frac{3}{6}}_{\frac{1}{2}}, \underbrace{\frac{4}{6}}_{\frac{2}{3}}, \frac{5}{6}, \underbrace{\frac{6}{6}}_{\frac{1}{1}}$

$\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(6) = 2$

Arithmetic functions, Möbius inversion formula

Def. A function $f: \mathbb{N}_+ \to \mathbb{C}$ is called

multiplicative if $[\gcd(m,n)=1 \Rightarrow f(mn)=f(m)f(n)]$

strongly multiplicative if $\forall m,n \in \mathbb{N}_+ \quad f(mn)=f(m)f(n)$.

Note: f multiplicative $\Rightarrow f(1\cdot 1)=f(1)^2 \Rightarrow \begin{cases} \text{either } f(1)=0 \Rightarrow \forall n \ f(n)=0 \\ \text{or } f(1)=1 \end{cases}$

Def. For any function $f: \mathbb{N}_+ \to \mathbb{C}$, let $\boxed{Z_f(s) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s}}$ be its formal generating (Dirichlet) series (s = formal variable).

Note: (1) writing each $n \in \mathbb{N}_+$ as $n = \prod_{p \in P} p^{a_p}$, then

- f multiplicative $\Rightarrow f(n) = f(1)\prod_p f(p^{a_p})$, $Z_f(s) = f(1)\prod_{p\in P}\left(1+\sum_{k\geq 1}\frac{f(p^k)}{p^{ks}}\right)$
- f strongly multiplicative $\Rightarrow f(n) = f(1)\prod_p f(p)^{a_p}$,

$$\boxed{Z_f(s) = f(1)\prod_{p\in P}\sum_{k\geq 0}\left(\frac{f(p)}{p^s}\right)^k = f(1)\prod_{p\in P}\frac{1}{1-\frac{f(p)}{p^s}}}$$

(2) **δ-function:** $\delta(n) := \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$, $Z_\delta(s)=1$

(3) **constant function:** $\mathbb{1}(n) := 1 \quad (\forall n \in \mathbb{N}_+)$, $Z_{\mathbb{1}}(s) = \underbrace{\sum_{n=1}^{\infty}\frac{1}{n^s}}_{\text{the zeta-function } \zeta(s)} = \prod_{p\in P}\frac{1}{1-\frac{1}{p^s}}$ ← Euler's formula

(4) **convolution $\longleftrightarrow$ product:** $Z_f(s)Z_g(s) = Z_h(s)$, where

$$h(n) := \sum_{ab=n} f(a)g(b) = \sum_{d\mid n} f(d)\,g\left(\frac{n}{d}\right)$$ (the **convolution** of f, g)

$(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$

notation: $h = f*g = g*f$

(5) $f * \mathbb{1} = \mathbb{1} * f = g$, $g(n) = \sum_{d\mid n} f(d)$, $Z_g(s) = Z_f(s)\underbrace{Z_{\mathbb{1}}(s)}_{\zeta(s)}$

(6) the **Möbius function** $\mu: \mathbb{N}_+ \to \mathbb{C}$; $\boxed{Z_\mu(s) = \frac{1}{\zeta(s)}}$

But $\frac{1}{\zeta(s)} = \prod_{p\in P}\left(1-\frac{1}{p^s}\right) = \sum_{n\geq 1}\frac{\mu(n)}{n^s} \Rightarrow \mu(n) = \begin{cases} 0 & \text{if } \exists p \in P,\ p^2 \mid n \\ (-1)^r & \text{if } n = p_1 \cdots p_r,\ r \geq 0,\ p_i \in P \text{ distinct} \end{cases}$

(7) Möbius inversion formula: if $f, g: \mathbb{N}_+ \longrightarrow \mathbb{C}$ and $\forall n \geq 1 \; g(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

If: $g = f * \mathbb{1} \Rightarrow Z_g = Z_f Z_{\mathbb{1}} = Z_f\, \zeta(s) \Rightarrow Z_f = \underbrace{\zeta(s)^{-1}}_{Z_\mu} Z_g \Rightarrow f = \mu * g$.

---

(8) If $a \in \mathbb{C}$, let $\sigma_a(n) := \sum_{d|n} \underbrace{d^a}_{e^{a \ln(d)}}$ (multiplicative)

$\sigma_a = \mathbb{1} * (n \longmapsto n^a) \Rightarrow Z_{\sigma_a}(s) = Z_{\mathbb{1}}(s)\, Z_{(n \mapsto n^a)}(s) = \zeta(s)\,\zeta(s-a)$

Exercise 1. Compute $\sum_{n \geq 1} \frac{\varphi(n)}{n^s} = Z_\varphi(s)$.

Exercise 2. Contemplate the following inversion formulas:

(a) $f, g: \mathbb{N} \longrightarrow \mathbb{C}$, $g(n) = \sum_{m \leq n} f(m) \Rightarrow f(n) = g(n) - g(n-1)$ $\left(\underbrace{\;=0 \text{ if } n=0\;}\right)$

(b) X finite set, $f, g: \{\text{subsets of } X\} \longrightarrow \mathbb{C}$

$$g(A) = \sum_{B \subseteq A} f(B) \Rightarrow f(A) = \sum_{B \subseteq A} (-1)^{|A|-|B|}\, g(B)$$

(c) $f, g: \mathbb{N}_+ \longrightarrow \mathbb{C}$, $g(n) = \sum_{d|n} f(d) \Rightarrow f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

Is there a common generalisation?

Exercise: For $n, r \in \mathbb{N}_+$, let $\varphi_r(n) := \left|\{(a_1, \dots, a_r) \mid 1 \leq a_i \leq n,\ \gcd(a_1, \dots, a_r, n) = 1\}\right|$ ($\varphi_1(n) = \varphi(n)$).

(a) Determine $\sum_{d|n} \varphi_r(d)$ and $Z_{\varphi_r}(s) = \sum_{n=1}^{\infty} \frac{\varphi_r(n)}{n^s}$.

(b) Give an explicit formula for $\varphi_r(n)$ in terms of the prime factorisation $n = p_1^{a_1} \cdots p_k^{a_k}$.

Euclidean quadratic rings

If $d \in \mathbb{Z}$, $\sqrt{d} \notin \mathbb{Z}$, then $\sqrt{d} \notin \mathbb{Q}$ and

$\mathbb{Q}(\sqrt{d}) = \{ a+b\sqrt{d} \mid a, b \in \mathbb{Q} \}$ is a field with involution

$\alpha = a+b\sqrt{d} \longmapsto \alpha' = a-b\sqrt{d}$ (a, b are uniquely determined by α)

the norm $N(\alpha) = \alpha\alpha' = a^2 - db^2$

satisfies: $N(\alpha)=0 \Leftrightarrow \alpha = 0$; $N(\alpha\beta) = N(\alpha)N(\beta)$; $\forall \alpha \in \mathbb{Q}$ $N(\alpha) = \alpha^2$

Exercise 1. If $d \in \{-1, -2, 2, 3\}$, then the subring

$\mathbb{Z}[\sqrt{d}] = \{ a+b\sqrt{2} \mid a, b \in \mathbb{Z} \}$ is a Euclidean domain with respect to $\alpha \longmapsto |N(\alpha)|$.

Exercise 2. (a) If $d \equiv 1 \pmod 4$, then $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ (the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and $\frac{1+\sqrt{d}}{2}$) is equal to

$\mathbb{Z}\cdot 1 + \mathbb{Z} \cdot \frac{1+\sqrt{d}}{2} = \left\{ \frac{a+b\sqrt{d}}{2} \;\middle|\; a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}$.

(b) If $d \in \{-3, -7, -11, 5, 13\}$, then $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ is a Euclidean domain with respect to $\alpha \longmapsto |N(\alpha)|$.

Exercise 3. Assume that A is a UFD, $f(X) = a_n X^n + \cdots + a_0 \in A[X]$, $a_0, a_n \neq 0$, $f\left(\frac{a}{b}\right) = 0$, where $a, b \in A \setminus \{0\}$ and $\gcd(a, b) = 1$.

Then: $a \mid a_0$ and $b \mid a_n$.

Cor. If $d \in \mathbb{Z}$, $\sqrt{d} \notin \mathbb{Z}$ and $d \equiv 1 \pmod 4$, then $\mathbb{Z}[\sqrt{d}]$ is not a UFD.

[Hint: take $b = 2$, $a = 1+\sqrt{d}$, $f(X) = X^2 - X + \frac{1-d}{4}$.]

Rmk. (1) The case $a_n = 1$ of Exercise 3 says that any UFD is integrally closed. In the above example, $\frac{1+\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$ is integral over $\mathbb{Z}[\sqrt{d}]$.

(2) $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ is not a Euclidean domain, but it is a UFD.

(3) $\mathbb{Z}[\sqrt{14}]$ is a Euclidean domain, but not with respect to $|N|$.

Ex: $\boxed{y^2+7=x^3 \qquad (x,y\in\mathbb{Z})}$ $\qquad (\pm1)^2+7=2^3$

$\gcd(x,y)^2 \mid \underbrace{(x^3-y^2)}_{7} \Rightarrow \gcd(x,y)=1$; moreover, $7\nmid x$

(mod 8): $y^2+7\equiv 0,3,7 \pmod 8$, $x^3=0,1,3,5,7 \pmod 8$ $(\Rightarrow x^3\not\equiv 1 \pmod 4 \Leftrightarrow x\not\equiv 1 \pmod 4$

Factorisation in the Euclidean domain $A=\mathbb{Z}\left[\frac{1+i\sqrt{7}}{2}\right]=\left\{\frac{a+bi\sqrt{7}}{2} \mid a,b\in\mathbb{Z},\ a\equiv b \pmod 2\right\}$

(norm: for $\alpha\in A$, $N(\alpha)=\alpha\bar{\alpha}$) $A^\times=\{\alpha\in A \mid N(\alpha)\in\mathbb{Z}^\times=\{\pm1\}\}=\{\pm1\}$ $(N(\alpha\beta)=N(\alpha)N$

$2=\frac{1+i\sqrt{7}}{2}\cdot\frac{1-i\sqrt{7}}{2}$; $N\left(\frac{1\pm i\sqrt{7}}{2}\right)=2$ prime $\Rightarrow \frac{1\pm i\sqrt{7}}{2}\in A$ irreducible

$x^3=y^2+7=(y+i\sqrt{7})(y-i\sqrt{7})$ let $d=\gcd(y+i\sqrt{7},\ y-i\sqrt{7})\in(A\setminus\{0\})/A^\times$

Divisibilities: $d^2\mid x^3$, $d\mid 2y$, $d\mid 2i\sqrt{7}\ (=(y+i\sqrt{7})-(y-i\sqrt{7}))$ (in A)

$\Rightarrow N(d)\mid x^3$, $N(d)\mid 4y^2$, $d\mid 28$ (in $\mathbb{Z}$), hence

$N(d)\mid \gcd(x^3,4y^2,28)=\gcd(x^3,4y^2,4)=\gcd(x^3,4)=\gcd(x^2,4)=\gcd(x,2)^2$

Case 1: $\boxed{2\nmid x,\ 2\nmid y}$ $N(d)=1\Rightarrow d=1$, hence

$y+i\sqrt{7}=u\alpha^3$, $\alpha\in A$, $u\in A^\times=\{\pm1\}$ $(\Rightarrow u=u^3)$. As a result,

$y\pm i\sqrt{7}=\left\{\begin{matrix}\alpha^3\\ \beta^3\end{matrix}\right\}$, $\beta\in A$ $(\beta=u\alpha)$. Write $\beta=\frac{a+bi\sqrt{7}}{2}$ $a,b\in\mathbb{Z}$, $2\mid(a-b)$

$y+i\sqrt{7}=\left(\frac{a+bi\sqrt{7}}{2}\right)^3=\frac{a^3-21ab^2}{8}+\frac{i\sqrt{7}}{8}(3a^2b-7b^3)$

$8y=a(a^2-21b^2)$, $\quad 8=b(3a^2-7b^2)$

If $2\mid a\Rightarrow 2\mid b$, $\quad 1=\frac{b}{2}\left(3\left(\frac{a}{2}\right)^2-7\left(\frac{b}{2}\right)^2\right)$, $\quad \frac{b}{2}=\pm1=3\left(\frac{a}{2}\right)^2-7$ — impossible

If $2\nmid a\Rightarrow 2\nmid b\Rightarrow b=\pm1$, $\pm8=3a^2-7$ — impossible

Conclusion: no solution with $2\nmid x$

Case 2: $\boxed{2\mid x,\ 2\nmid y}$ $\frac{y\pm i\sqrt{7}}{2}\in A\Rightarrow 2\mid d$; as $N(d)\mid 4$, we have $d=2$

Write $x=2z$ $(z\in\mathbb{Z})$; $\frac{y+i\sqrt{7}}{2}\cdot\frac{y-i\sqrt{7}}{2}=2z^3=\left(\frac{1+i\sqrt{7}}{2}\right)\left(\frac{1-i\sqrt{7}}{2}\right)z^3$

$\gcd\left(\frac{y\pm i\sqrt{7}}{2},\frac{y-i\sqrt{7}}{2}\right)=\frac{d}{2}=1$, $\quad 2\nmid\frac{y\pm i\sqrt{7}}{2}\Rightarrow \exists u\in A^\times\ \exists\alpha\in A$

(possibly after $y\mapsto -y$) $\boxed{\frac{y+i\sqrt{7}}{2}=u\,\frac{1+i\sqrt{7}}{2}\alpha^3=\underbrace{\frac{1+i\sqrt{7}}{2}\beta^3}_{u^3=1}}$ $\beta=u\alpha\in A$

Write $\beta=\frac{a+bi\sqrt{7}}{2}$, $2\mid(a-b)$; then

$$\frac{a^3-21a^2b-21ab^2+49b^3}{16}+\boxed{\frac{i\sqrt{7}}{16}(a^3+3a^2b-21ab^2-7b^3)}$$

$\Rightarrow 8y=a^3-21a^2b-21ab^2+49b^3$

$8=a^3+3a^2b-21ab^2-7b^3=8\left(\frac{a+b}{2}\right)^3-6\left(\frac{a+b}{2}\right)b^2+2b^3\Big)$

let $a'=\frac{a+b}{2}\in\mathbb{Z}$; then $\boxed{a'^3-6a'b+2b^3=1}$ Thue equation

the obvious solution $a'=1$, $b=0$ corresponds to $a=2$, $b=0$, $\beta=1$,

$y=1$, $x=2$.

Def. A **Thue equation** is a diophantine equation

$$F(x,y)=m \qquad (x,y\in\mathbb{Z}),$$

where $F(x,y)=a_0x^n+a_1x^{n-1}y+\cdots+a_n\in\mathbb{Z}[x,y]$ is homogeneous of $\deg(F)=n$ and $m\in\mathbb{Z}\setminus\{0\}$.

Thm (Thue, 1909) If F is irreducible in $\mathbb{Q}[x,y]$ ($\Leftrightarrow$ $a_0T^n+a_1T^{n-1}+\cdots+a_n$ is irreducible in $\mathbb{Z}[T]$) and $n\geq 3$, then, for each $m\in\mathbb{Z}\setminus\{0\}$,

$$\left|\{(u,v)\in\mathbb{Z}^2 \mid F(u,v)=m\}\right|<\infty.$$

In Ex: $y^2+7=x^3$, the case $2\nmid x$ (resp. $2\mid x$) led to a reducible (resp. irreducible) Thue equation of $\deg=3$.

Fact (Landau–Ostrowski) For each $k\in\mathbb{Z}\setminus\{0\}$ the diophantine equation $y^2+k=x^3$ can be reduced to a finite number of Thue equations of $\deg=3$.

Ex: $\boxed{y^2-18=x^3 \quad (x,y\in\mathbb{Z})}$

$(y+3\sqrt{2})(y-3\sqrt{2})$

$\underbrace{(\pm 19)^2}_{361}-\underbrace{18}_{2\cdot 3^2}=\underbrace{7^3}_{343}$

$A=\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\}$ Euclidean domain with respect to $|N|$, where $N(\underbrace{\alpha}_{a+b\sqrt{2}})=\alpha\alpha'=a^2-2b^2$ $\quad((a+b\sqrt{2})'=a-b\sqrt{2})$

$(19+3\sqrt{2})(19-3\sqrt{2})=7^3$, $\quad (3+\sqrt{2})(3-\sqrt{2})=7 \quad (3^2-2=7)$

$\nwarrow\ \nearrow$ irreducible in A, since $N(3\pm\sqrt{2})=7$ is a prime

$N(\alpha\beta)=N(\alpha)N(\beta)$

$(3\pm\sqrt{2})^3=45\pm 29\sqrt{2}$

Uniqueness of factorisation: $19+3\sqrt{2}=(3-\sqrt{2})^3\underbrace{(3+2\sqrt{2})}_{(1+\sqrt{2})^2\in A^\times}$

Fact (proof later): $\underbrace{\mathbb{Z}[\sqrt{2}]^\times}_{\{\alpha\in\mathbb{Z}[\sqrt{2}] \mid N(\alpha)\in\mathbb{Z}^\times=\{\pm 1\}\}}=\{\pm(1+\sqrt{2})^n \mid n\in\mathbb{Z}\}$

If $d=(y+3\sqrt{2},\ y-3\sqrt{2})$ in $A=\mathbb{Z}[\sqrt{2}]$, then $d^2\mid x^3$, $d\mid\underbrace{(y+3\sqrt{2})\pm(y-3\sqrt{2})}_{2y,\ 6\sqrt{2}}$

$N(d)\mid \gcd(x^3,4y^2,72)$. But $2\nmid xy$, $\gcd(x,y)^2\mid x^3-y^2=18 \Rightarrow \gcd(x,y)\mid 3$

If $y=3y'$ and $x=3x'$, then $y'^2-2=3x'^3$ — impossible (mod 3). So $\gcd(x,y)=1 \Rightarrow N(d)=1 \Rightarrow d=1 \Rightarrow y+3\sqrt{2}=u\alpha^3$, $u\in A^\times$, $\alpha\in A$.

But $A^\times/A^{\times 3}=\{1,(1+\sqrt{2})^{\pm 1}\}$ $\Rightarrow$ get 3 Thue equations from $y+3\sqrt{2}=(a+b\sqrt{2})^3\cdot\{\sqrt{2}\pm 1,\ 1\}$. One of them is reducible, two aren't.

Arithmetic properties of $\mathbb{Z}[i]$

$\Updownarrow$

(——— " ———) x^2+y^2 over $\mathbb{Z}$

Arithmetic of $\mathbb{Z}[i] = \{\alpha = a+bi \mid a, b \in \mathbb{Z}\}$:

(i) $\mathbb{Z}[i]$ is a Euclidean domain ($\Rightarrow$ a UFD) with respect to the norm $N(\alpha) = \alpha\overline{\alpha} = a^2+b^2$ ($N(\alpha) \in \mathbb{N}$, $N(\alpha) \neq 3 \pmod 4$)

(ii) $N(\alpha\beta) = N(\alpha)\,N(\beta)$

(iii) $\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i] \mid \underbrace{N(\alpha)}_{\in \mathbb{N}} \in \mathbb{Z}^\times = \{\pm 1\}\} = \{i^k \mid k \in \mathbb{Z}/4\mathbb{Z}\} = \mu_4(\mathbb{C})$ $\Leftrightarrow N(\alpha) = 1$

(iv) If $N(\alpha) = p$ is a prime, then α is irreducible in $\mathbb{Z}[i]$

(v) If $\alpha \in \mathbb{Z}[i]$ is irreducible, then $\alpha \mid p$ for some prime p (unique)

(indeed, $\alpha \mid \underbrace{N(\alpha)}_{\in \mathbb{Z}_{\geq 2}} = \prod p_i^{r_i}$ $\xRightarrow{\text{Euclid's Lemma in } \mathbb{Z}[i]}$ $\exists i$ $\alpha \mid p_i$).

(vi) $2 = (1+i)(1-i) = (1+i)^2(-i)$, $1+i$ irreducible (since $N(1+i) = 2$).

(vii) If $p \equiv 3 \,[4]$ is a prime, then p is irreducible in $\mathbb{Z}[i]$

(otherwise $p = \alpha\beta$, $\alpha, \beta \notin \mathbb{Z}[i]^\times \Rightarrow \underbrace{N(\alpha)}_{>1}\underbrace{N(\beta)}_{>1} = N(p) = p^2$

$\Rightarrow N(\alpha) = N(\beta) = p \equiv 3 \,[4]$ – false)

(viii) If $p \equiv 1 \,[4]$ is a prime, then $\exists\, a \in \mathbb{Z}$ $a^2 \equiv -1 \,[p]$;

$p \mid (a^2+1) = (a+i)(a-i)$, $p \nmid (a \pm i)$ $\xRightarrow{\text{Euclid's Lemma in } \mathbb{Z}[i]}$ p not irreducible in $\mathbb{Z}[i]$

Thus $p = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$, $p^2 = N(p) = \underbrace{N(\alpha)}_{>1}\underbrace{N(\beta)}_{>1} \Rightarrow$

$N(\alpha) = N(\beta) = p \Rightarrow \beta = \overline{\alpha}$, $\alpha = a+bi$, $a^2+b^2 = p$.

Summary: $\mathbb{Z}[i]$ is a UFD, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{i^k \mid k \in \mathbb{Z}/4\mathbb{Z}\}$,

$$\left\{\begin{matrix}\text{irreducible elements} \\ \text{of } \mathbb{Z}[i]\end{matrix}\right\} = \{i^k(1+i)\} \cup \{p \mid p \equiv 3 \,[4] \text{ prime}\} \cup \{\pi_p^k, \overline{\pi_p}^k \mid p \equiv 1 \,[4] \text{ prime}\},$$

$N(\cdot) = 2$ $\quad$ $N(\cdot) = p^2$ $\quad$ $N(\cdot) = p$

where we fix $a, b \in \mathbb{Z}$ such that $a^2+b^2 = p \equiv 1 \,[4]$ and let $\pi_p = a+bi$ $(\pi_p \neq \overline{\pi_p})$

Unique factorisation: $\forall \alpha \in \mathbb{Q}(i)^\times$

$$\alpha = i^k (1+i)^a \prod_{p\equiv 1[4]} \pi_p^{b_p} \overline{\pi_p}^{c_p} \prod_{p\equiv 3[4]} p^{d_p}, \qquad \underbrace{k \in \mathbb{Z}/4\mathbb{Z};\ a, b_p, c_p, d_p \in \mathbb{Z}}_{\text{unique}}$$

$$N(\alpha) = 2^a \prod_{p\equiv 1[4]} p^{b_p+c_p} \prod_{p\equiv 3[4]} p^{2d_p}$$

$$\alpha \in \mathbb{Z}[i]^\times \iff a,\ b_p, c_p, d_p \geq 0 \quad (\forall p)$$

$$N(\alpha) \in \mathbb{Z} \iff a,\ b_p+c_p,\ d_p \geq 0 \quad (\forall p)$$

If $N(\alpha) \in \mathbb{Z}$, then $\alpha' := (1+i)^a \prod_{p\equiv 1[4]} \pi_p^{b_p+c_p} \prod_{p\equiv 3[4]} p^{d_p} \in \mathbb{Z}[i]^\times$ and $N(\alpha') = N(\alpha)$.

Representability of integers by the quadratic form $f = x^2+y^2$

We want to determine:

$$S^+_{\mathbb{Q}}(f) = \{n \in \mathbb{N}_+ \mid \exists u, v \in \mathbb{Q} \quad n = u^2+v^2\} = \{N(\alpha) \mid \alpha \in \mathbb{Q}(i)^\times, N(\alpha) \in \mathbb{Z}\}$$

$$\cup \qquad\qquad \cup$$

$$S^+(f) = \{- \text{ " } - \mid \exists u, v \in \mathbb{Z} \quad - \text{ " } -\} = \{N(\alpha) \mid \alpha \in \mathbb{Z}[i]^\times\}$$

$$\cup$$

$$S^+_{\text{prim}}(f) = \{- \text{ " } - \mid - \text{ " } -,\ \gcd(u,v)=1,\ n=u^2+v^2\} = \{N(\alpha) \mid \alpha \in \mathbb{Z}[i]^\times,\ \forall p \text{ prime } p \nmid \alpha\}$$

Note: (a) $S^+(f) = \bigcup_{d\geq 1} d^2\, S^+_{\text{prim}}(f)$ (write $\alpha = d\beta$, $\forall p$ prime $p \nmid \beta$)

(b) $\alpha \in \mathbb{Z}[i]^\times$ satisfies $[\forall p \text{ prime } p \nmid \alpha] \iff \{a \leq 1,\ \forall p \equiv 3[4]\ d_p = 0,\ \{\forall p \equiv 1[4]\ b_p = 0 \text{ or } c_p = 0.\}\}$

The above formulas imply:

Thm. $S^+_{\mathbb{Q}}(f) = \{n \in \mathbb{N}_+ \mid \forall p \equiv 3[4] \quad 2 \mid v_p(n)\} = S^+(f)$

$$S^+_{\text{prim}}(f) = \underbrace{\{n \in \mathbb{N}_+ \mid v_2(n) \leq 1,\ \forall p \equiv 3[4] \quad v_p(n) = 0\}}_{\{n \in \mathbb{N}_+ \mid \exists z \in \mathbb{Z} \quad z^2 \equiv -1\ [n]\}} \quad (\text{proof - later})$$

Note: (i) $m, n \in S^+(f) \implies mn \in S^+(f)$ (since $N(\alpha\beta) = N(\alpha)N(\beta)$)

(ii) $m, n \in S^+(f)$, $(m,n)=1 \overset{\text{Thm}}{\implies} m, n \in S^+(f)$ (requires the UFD property)

(iii) $mn \in S^+_{\text{prim}}(f) \implies m, n \in S^+_{\text{prim}}(f)$ (— " —)

Question 1. Is it possible to prove directly $S^+_{\mathbb{Q}}(f) = S^+(f)$, i.e., that if $n \in \mathbb{N}_+$ is a sum of two rational squares, it is a sum of two integral squares ?

Question 2. What happens if we replace $(x^2+y^2, \mathbb{Z}[i])$ by $(x^2-xy+y^2, \mathbb{Z}[\underbrace{\frac{-1+i\sqrt{3}}{2}}_{\xi_3}])$ or by $(x^2+2y^2, \mathbb{Z}[i\sqrt{2}])$? And what about x^2+3y^2 ?

The number of representations by $f = x^2+y^2$

Def. For $n \in \mathbb{N}$, let $r_f(n) := |\{(u,v) \in \mathbb{Z}^2 \mid u^2+v^2 = n\}| = |\{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = n\}|$

$w_f := |\mathbb{Z}[i]^\times| = 4$.

Analytic formulation of unique factorisation:

in $\mathbb{Z}$: write $n \in \mathbb{N}_+$ as $p_1^{r_1} \cdots p_k^{r_k}$; then (s = formal variable)

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

in $\mathbb{Z}[i]$: $\frac{1}{w_f} \sum \frac{r_f(n)}{n^s} = \sum_{\alpha \in (\mathbb{Z}[i] - \{0\})/\mathbb{Z}[i]^\times} \frac{1}{N(\alpha)^s} = \prod_{\pi \in \{\text{irred. elts of } \mathbb{Z}[i]\}/\mathbb{Z}[i]^\times} \left(1 - \frac{1}{N(\pi)^s}\right)^{-1} =$

$= \prod_{\pi \mid 2} \prod_{\pi \mid p \equiv 1[4]} \prod_{\pi \mid p \equiv 3[4]} (\quad)^{-1} = (1-2^{-s})^{-1} \prod_{p \equiv 1[4]} (1-p^{-s})^{-2} \prod_{p \equiv 3[4]} (1-p^{-2s})^{-1} =$

modulo $\mathbb{Z}[i]^\times$ → $\pi \mid 2$: $(1+i)$, $N = 2$; $\pi \mid p \equiv 1[4]$: $\pi_p, \overline{\pi_p}$, $N = p$; $\pi \mid p \equiv 3[4]$: (p), $N = p^2$

$$= \underbrace{\prod_p (1-p^{-s})^{-1}}_{\zeta(s)} \underbrace{\prod_{p \equiv 1[4]} (1-p^{-s})^{-1} \prod_{p \equiv 3[4]} (1+p^{-s})^{-1}}$$

$$L(s) = \prod_{p \neq 2} \left(1 - (-1)^{\frac{p-1}{2}} p^{-s}\right)^{-1} = \sum_{\substack{n \geq 1 \\ 2 \nmid n}} \frac{(-1)^{\frac{n-1}{2}}}{n^s}$$

$= 1 - 3^{-s} + 5^{-s} - 7^{-s} + \cdots$

Cor. $\forall n \in \mathbb{N}_+ \quad r_f(n) = \sum_{2 \nmid d \mid n} (-1)^{\frac{d-1}{2}}$

Question 3. What about $r_f(n)$ for $f = x^2-xy+y^2$, x^2+2y^2 or x^2+3y^2 ?

Congruences for squares modulo 2^r

Prop 1. $\forall x \in \mathbb{Z} \quad x^2 \equiv 0, 1 \ [4]$. **Pf:** $2 \nmid x \Rightarrow 2^2 \mid x^2$

$2 \nmid x \Rightarrow x \equiv \pm 1 \ [4] \Rightarrow x^2 \equiv (\pm 1)^2 \equiv 1 \ [4]$.

Cor. For $x_j \in \mathbb{Z}$,

$x_1^2 + x_2^2 \not\equiv 3 \ [4]$

$x_1^2 + x_2^2 \equiv 0 \ [4] \iff 2 \mid x_1, 2 \mid x_2$

$x_1^2 + x_2^2 \equiv 2 \ [4] \iff 2 \nmid x_1, 2 \nmid x_2$

$x_1^2 - x_2^2 \not\equiv 2 \ [4]$

Exercise. $\{x_1^2 - x_2^2 \mid x_j \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid n \not\equiv 2 \ [4]\}$.

Prop. 2. $\forall x \in \mathbb{Z} \quad x^2 \equiv 0, 1, 4 \ [8]$. **Pf:** $2 \mid x \Rightarrow 2^2 \mid x^2 \Rightarrow x^2 \equiv 0, 4 \ [8]$

$2 \nmid x \Rightarrow x \equiv \pm 1, \pm 3 \ [8] \Rightarrow x^2 \equiv (\pm 1)^2, (\pm 3)^2 \equiv 1 \ [8]$

Cor. $x_1^2 + x_2^2 + x_3^2 \equiv 3 \ [8] \iff 2 \nmid x_1, 2 \nmid x_2, 2 \nmid x_3$

$(x_j \in \mathbb{Z})$ $x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \ [8]$

$x_1^2 + x_2^2 + x_3^2 \equiv 0 \ [4] \iff 2 \mid x_1, 2 \mid x_2, 2 \mid x_3$

$\Rightarrow x_1^2 + x_2^2 + x_3^2 \neq 4^k(8m+7)$

---

the three squares theorem (Gauss): $\{x_1^2 + x_2^2 + x_3^2 \mid x_j \in \mathbb{Z}\} = \{n \in \mathbb{N} \mid n \neq 4^k(8m+7)\}$

(difficult)

---

the four squares theorem (Lagrange): $\{x_1^2 + x_2^2 + x_3^2 + x_4^2 \mid x_j \in \mathbb{Z}\} = \mathbb{N}$

(easier)

Prop. 3. For $a \in \mathbb{Z}$, $2 \nmid a$, the congruence $x^2 \equiv a \ [2^r]$ has a solution $x \in \mathbb{Z}$ let $r \geq 3$.

$\Uparrow$

— " — $x^2 \equiv a \ [2^3]$ — " —

$\Uparrow$ ← Prop. 2.

$a \equiv 1 \ [8]$.

Pf. By induction, we need to show: if $r \geq 3$, $2 \nmid a$,

$x^2 = a + 2^r b \Rightarrow \exists y \in \mathbb{Z}$ $x' := x + 2^{r-1} y$ satisfies $x'^2 = a + 2^{r+1} b'$ $(b, b' \in \mathbb{Z})$

Indeed, $x'^2 = \underbrace{x^2 + 2^r xy}_{a + 2^r(xy+b)} + 2^{r+1}(2^{r-3} y^2)$

But $2 \nmid a \Rightarrow 2 \nmid x$, so we just take $y = b \Rightarrow 2 \mid (xy+b)$.

Question: if $a \equiv 1 \ [8]$, what is the number of solutions (mod 2^r) of the congruence

$x^2 \equiv a \ [2^r]$ $(r \geq 3)$?

[**Hint:** consider first the case $a = 1$]

The statement and the proof of Prop. 3 are special instances of Hensel's Lemma.

Congruences $x^2 \equiv a \ [p]$, $p \neq 2$ prime

Notation: $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, $a \longmapsto \overline{a} = a \pmod p$ — the canonical projection

$(p \nmid a \iff \overline{a} \in \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\})$

Goal: study $QR = \{\text{quadratic residues } \pmod p\} = \mathbb{F}_p^{\times 2} = \{x^2 \pmod p \mid x \in \mathbb{Z},\ p \nmid x\}$

$NR = \{-\!\!-\!\!-\text{ nonresidues }-\!\!-\!\!-\} = \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$

Basic observations: for $x, y \in \mathbb{Z}$,

$$x^2 \equiv y^2 \ [p] \iff p \mid (x+y)(x-y) \overset{\text{Euclid's Lemma}}{\iff} p \mid (x+y) \text{ or } p \mid (x-y) \iff x \equiv \pm y \ [p].$$

Cor: $\mathbb{F}_p^\times = \{\pm\overline{1}, \pm\overline{2}, \dots, \pm\overline{\tfrac{p-1}{2}}\} \Longrightarrow \mathbb{F}_p^{\times 2} = \{\underbrace{\overline{1^2}, \overline{2^2}, \dots, \overline{(\tfrac{p-1}{2})^2}}_{\text{distinct}}\}$

$$\Rightarrow |QR| = |NR| = \frac{1}{2}|\mathbb{F}_p^\times| = \frac{p-1}{2}.$$

Numerical experiments

p	$x^2 = 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121 \pmod p$
3	$\overline{1}$
5	$\overline{1}, \overline{-1}$
7	$\overline{1}, \overline{-3}, \overline{2}$
11	$\overline{1}, \overline{4}, \overline{-2}, \overline{5}, \overline{3}$
13	$\overline{1}, \overline{4}, \overline{-4}, \overline{3}, \overline{-1}, \overline{-3}$
17	$\overline{1}, \overline{4}, \overline{-8}, \overline{-1}, \overline{8}, \overline{2}, \overline{-2}, \overline{-4}$
19	$\overline{1}, \overline{4}, \overline{9}, \overline{-3}, \overline{6}, \overline{-2}, \overline{-8}, \overline{7}, \overline{5}$
23	$\overline{1}, \overline{4}, \overline{9}, \overline{-7}, \overline{2}, \overline{-10}, \overline{3}, \overline{-5}, \overline{-11}, \overline{8}, \overline{6}$

Symmetry:

$p \equiv 1 \ [4]$	$\mathbb{F}_p^{\times 2}$
5	$\overline{\pm 1}$
13	$\overline{\pm 1}, \overline{\pm 3}, \overline{\pm 4}$
17	$\overline{\pm 1}, \overline{\pm 2}, \overline{\pm 4}, \overline{\pm 8}$

Asymmetry:

$p \equiv 3 [4]$	$\mathbb{F}_p^{\times 2}$
3	$\overline{1}$
7	$\overline{1}, \overline{2}, \overline{-3}$
11	$\overline{1}, \overline{-2}, \overline{3}, \overline{4}, \overline{5}$
19	$\overline{1}, \overline{-2}, \overline{-3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{-8}, \overline{9}$
23	$\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{-5}, \overline{6}, \overline{-7}, \overline{8}, \overline{9}, \overline{-10}, \overline{-11}$

There seem to be relatively few signs "$-$" in this table. Equivalently, there seem to be more quadratic residues $(\mathrm{mod}\ p)$ in the interval $0 < a < \frac{p}{2}$ than for $\frac{p}{2} < a < p$:

Quadratic residues $(\mathrm{mod}\ p)$, $p \equiv 3 [4]$:

p	I: $0 < a < \frac{p}{2}$	II: $\frac{p}{2} < a < p$	$\lvert I \rvert$	$\lvert II \rvert$	$\lvert I \rvert - \lvert II \rvert$
3	1		1	0	1
7	1, 2	4	2	1	1
11	1, 3, 4, 5	9	4	1	3
19	1, 4, 5, 6, 7, 9	11, 16, 17	6	3	3
23	1, 2, 3, 4, 6, 8, 9	12, 13, 16, 18	7	4	3

Is there a similar asymmetry for QR $(\mathrm{mod}\ p)$ if $p \equiv 1 [4]$?

Quadratic residues $(\mathrm{mod}\ p)$, $p \equiv 1 [4]$:

p	I: $0 < a < \frac{p}{4}$	II: $\frac{p}{4} < a < \frac{p}{2}$	$\lvert I \rvert$	$\lvert II \rvert$	$\lvert I \rvert - \lvert II \rvert$
5	1		1	0	1
13	1, 3	4	2	1	1
17	1, 2, 4	8	3	1	2
29	1, 4, 5, 6, 7	9, 13	5	2	3
37	1, 3, 4, 7, 9	10, 11, 12, 16	5	4	1
41	1, 2, 4, 5, 8, 9, 10	16, 18, 20	7	3	4

Does this asymetry persist ? Yes !

Does it have a scientific explanation ? Yes !

Which one ? Stay tuned !

We first turn to the question of symmetry of QR.

Numerical experiments suggest that

$[\, a \in \mathbb{F}_p^{\times 2} \iff -a \in \mathbb{F}_p^{\times 2} \,]$ $(\iff -1 \in \mathbb{F}_p^{\times 2})$ holds for

$\underbrace{p = 5, 13, 17, \dots}_{p \equiv 1\,[4]}$, but not for $\underbrace{p = 3, 7, 11, 19, 23, \dots}_{p \equiv 3\,[4]}$.

This is, indeed, the case:

Prop. Let $p \neq 2$ be a prime.

$\underbrace{x^2 \equiv -1\,[p] \text{ has a solution } x \in \mathbb{Z}}_{-1 \in \mathbb{F}_p^{\times 2}} \iff p \equiv 1\,[4]$.

Pf. $(\Rightarrow)$ If $x^2 \equiv -1\,[p]$, then $1 \equiv x^{p-1} \equiv (x^2)^{\frac{p-1}{2}} \equiv \underbrace{(-1)^{\frac{p-1}{2}}}_{\pm 1}\,[p]$

$\Downarrow 1 \not\equiv -1\,[p]$

$1 = (-1)^{\frac{p-1}{2}} \Rightarrow p \equiv 1\,[4]$.

$(\Leftarrow)$ Elementary method: use

Wilson's Thm: p prime $\Rightarrow (p-1)! \equiv -1\,[p]$

(Special case $G = \mathbb{F}_p^\times$ of: $\forall (G, \cdot)$ finite abelian group

$$\prod_{g \in G} g = \prod_{\{g, g^{-1}\},\ g \neq g^{-1}} \underbrace{(g \cdot g^{-1})}_{1} \cdot \prod_{g = g^{-1}} g = \prod_{\substack{g \in G \\ g = g^{-1} \iff g^2 = 1}} g$$

)

If $p = 4k+1$, then $-1 \equiv (4k)! \equiv 1 \cdot 2 \cdots (2k) \underbrace{(2k+1)}_{\equiv -2k} \cdots \underbrace{(4k)}_{\equiv -1} \equiv (-1)^{2k} ((2k)!)^2 \equiv (2k!)^2\,[p]$

Reformulation: if $p \neq 2$ is a prime dividing n^2+1 $(n \in \mathbb{Z}) \Rightarrow p \equiv 1\,[4]$.

Exercise ✱. Use this property to show: (1) $|P \cap (4\mathbb{Z}+1)| = \infty$.

(2) If $a, b \in \mathbb{Z}$, $(a,b) = 1$ and $p \neq 2$ is a prime dividing a^2+b^2, then $p \equiv 1\,[4]$.

More scientific approach to $\Leftarrow$

Recall: (1) $|\mathbb{F}_p^\times| = p-1 \Rightarrow \forall a \in \mathbb{F}_p^\times \quad a^{p-1} = 1 \in \mathbb{F}_p$.

(2) K field, $f \in K[X] \setminus \{0\} \Rightarrow |\{\alpha \in K \mid f(\alpha) = 0\}| \leq \deg(f)$

(Pf: easy induction on $\deg(f)$).

Cor. If p is a prime, $f \in \mathbb{F}_p[X] \setminus \{0\} \Rightarrow f(x) \equiv 0 \ [p]$ has at most $\deg(f)$ solutions $(\mathrm{mod}\, p)$.

Back to $x^2 \ (\mathrm{mod}\, p)$, $p \neq 2$ prime

Prop. (1) $X^{p-1} - 1 = \underbrace{\prod_{a \in \mathbb{F}_p^\times} (X-a)}_{f(X)} \in \mathbb{F}_p[X]$.

(2) $X^{\frac{p-1}{2}} - 1 = \underbrace{\prod_{a \in \mathbb{F}_p^{\times 2}} (X-a)}_{f_+(X)}$, $X^{\frac{p-1}{2}} + 1 = \underbrace{\prod_{a \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}} (X-a)}_{f_-(X)} \in \mathbb{F}_p[X]$.

Pf. (1) Each $a \in \mathbb{F}_p^\times$ is a root of $X^{p-1} - 1 \Rightarrow f \mid (X^{p-1} - 1)$ in $\mathbb{F}_p[X]$

(f: monic, $\deg = p-1$) $\Rightarrow$ equality

(2) Each element $a = b^2 \in \mathbb{F}_p^{\times 2}$ $(b \in \mathbb{F}_p^\times)$ is a root of $X^{\frac{p-1}{2}} - 1$, hence

$f_+ \mid (X^{\frac{p-1}{2}} - 1)$ in $\mathbb{F}_p[X]$ $\overset{\text{as in (1)}}{\Longrightarrow}$ equality. Therefore

$$X^{\frac{p-1}{2}} + 1 = (X^{p-1} - 1) / (X^{\frac{p-1}{2}} - 1) = f / f_+ = f_-.$$

Cor 1. For $a \in \mathbb{F}_p^\times$, we have:

$a \in \mathbb{F}_p^{\times 2} \iff a^{\frac{p-1}{2}} = 1 \in \mathbb{F}_p$

$a \notin \mathbb{F}_p^{\times 2} \iff a^{\frac{p-1}{2}} = -1 \in \mathbb{F}_p$.

Cor 2 (the case $a = -1$) $-1 \in \mathbb{F}_p^{\times 2} \iff (-1)^{\frac{p-1}{2}} \equiv 1 \ [p] \iff (-1)^{\frac{p-1}{2}} = 1 \iff p \equiv 1 \ [4]$.

($-1 \not\equiv 1 \ [p]$)

In terms of the **Legendre symbol** defined for $b \in \mathbb{Z}$ as

$$\left(\frac{b}{p}\right) = \begin{cases} 0 & p \mid b \\ 1 & p \nmid b, \ x^2 \equiv b \ [p] \text{ has a solution } (\iff \overline{b} \in \mathbb{F}_p^{\times 2}) \\ -1 & p \nmid b, \ \text{—"— —"— no solution } (\iff \overline{b} \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}), \end{cases}$$

Cor 1 states that

(+ the trivial case $p \mid b$)

$$\boxed{\forall b \in \mathbb{Z} \quad \left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \ (\mathrm{mod}\, p)}$$

(Euler's criterion)

Rmk. If $p = 4k+1$ and if $a \in \mathbb{F}_p^\times$ is any root of $X^{\frac{p-1}{2}} + 1 = X^{2k} + 1$, then $b := a^k \in \mathbb{F}_p^\times$ is a root of $X^2 + 1$, hence $b^2 = -1$ in $\mathbb{F}_p$.

This is an explicit version of the above pf of Cor. 2.