NT. Division & Residue. Day 1

CRT: For pairwise coprime $(a_1, a_2, \cdots, a_n)$.

$\exists$ unique solution in $\{1, 2, \cdots, \prod a_i\}$

for $x \equiv b_i \ (a_i)$ $\forall i$ for any $b_i \in \mathbb{Z}$.

Proof: $\exists \alpha_i, \beta_i, i = 1, 2, \cdots, n$ s.t.

$$\alpha_i a_i + \beta_i \prod_{j \neq i} a_j = 1.$$

Then let $x = \sum_{i=1}^{n} b_i \beta_i \prod_{j \neq i} a_j$ ✓.

Unique: ✓.

$\tau(n) = |d : d \mid n|$, $\tau(p^k) = k+1$.

If $(m,n) = 1$. $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$.

Then $\tau(mn) = \prod(\alpha_i + 1) \prod(\beta_j + 1)$
$= \tau(m)\tau(n)$.

$\varphi(n) = |m : (m,n) = 1, 1 \le m \le n|$.

By CRT, multiplicative

$\sigma(n) = \sum_{d \mid n} d$.

If f multiplicative,

$g(mn) = \sum_{d \mid mn} f(d) = \cdots = \sum_{d \mid m} f(d) \sum_{d \mid n} f(d)$.

$n = \sum_{d \mid n} \varphi(d)$.

5. Division Algo: ~~Remainder~~ algo.

$\exists!$ poly f of deg n, then

$(x-\alpha)\, g(\alpha) \equiv 0\ (n)$.

$g(\alpha)$

Lagrange thm: p prime, $p \nmid a_n$,

$f(x) = a_0 + \cdots + a_n x^n$.

$f(x) \equiv 0\ (p)$ $\leq n$ sols mod p.

6. $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclic:

$\sum_{d \mid p-1} N_d = p-1 = \sum_{d \mid p-1} \varphi(d)$.

If $N_{p-1} = 0$, then $N_{d'} > \varphi(d')$ for some d'.

~~But say $\{x, x^2, \ldots, x^{d'}\}$ of deg d'.~~

~~$x^d - 1\ (p)$~~ $\langle \alpha \rangle = \{1, \alpha, \ldots, \alpha^{d'-1}\} \subseteq G$,

$\varphi(d')$ elements of order d.

$N_{d'} > \varphi(d')$, so $\exists$ element of order d outside, so $x^d - 1$ has $\geq d+1$ roots, 矛盾.

Residue.

1. Euler's Criteria.

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

proof: If $\left(\frac{a}{p}\right)=1$, then $a \equiv x^2 (p)$.

$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 (p)$. ✓.

Also exactly $\frac{p-1}{2}$ QR and $\frac{p-1}{2}$ NQR

SOV

$\downarrow$

$x^{\frac{p-1}{2}} - 1 \equiv 0 (p)$ $\leq \frac{p-1}{2}$ sols.

But $x^2 \equiv y^2 (p) \iff x = \pm y (p)$

So $\frac{p-1}{2}$ exactly sols. $\square$

Gauss's lemma:

$\left(\frac{p-1}{2}\right)! \, a^{\frac{p-1}{2}}$

$\equiv \prod \varepsilon_i c_i \equiv \left(\frac{p-1}{2}\right)! \cdot \left(\prod \varepsilon_i\right)$

where write $ax \equiv \varepsilon_i c_i$,

$c_i = \pm 1$

$\varepsilon_i \in \{1, 2, \dots, \frac{p-1}{2}\}$.

$x = \{1, 2, \dots, \frac{p-1}{2}\}$.

$ax \equiv ay (p)$ $\iff$ $x \equiv y (p)$; $ax \equiv -ay (p) \iff x + y \equiv 0 (p)$ so ε_i run through $\{1, 2, \dots, \frac{p-1}{2}\}$.

Jacobi Symbol

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right) \quad ; p_i \text{ odd} ; \left(\frac{a}{1}\right) = 1 .$$

$$\left(\frac{-1}{n}\right) \equiv (-1)^{\frac{n-1}{2}} .$$

$$\left(\frac{2}{n}\right) \equiv (-1)^{\frac{n^2-1}{8}}$$

$(2, 15)$

NT 2021.

P1, SI. Euler's criterion.

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \ (p)$$

If $\quad x$ primitive root $\Rightarrow x^{\frac{p-1}{2}} \not\equiv 1 \ (p)$

$\Rightarrow$ NQR.

$$\phi(p-1) = \phi(2^{2^k}) = 2^{2^k-1} = \frac{p-1}{2}.$$

$\mathbb{Z}/p\mathbb{Z}$ cyclic.

$\phi(p-1) = \frac{p-1}{2}$ so exactly NQR.

as NQR $\frac{p-1}{2}$ must have

$$\cancel{2^{2^{2^k}} \equiv 3^{2^{2^k-1}} \ (p)}.$$

$$\left(\frac{3}{p}\right) = (-1)^{\frac{(3-1)(p-1)}{4}} \left(\frac{p}{3}\right)$$

$$= \left(\frac{p}{3}\right) = -1. \checkmark$$

NT 2021

P4, SI, II

If $p^k | N$ for some $k \geq 1$.

$$N = \binom{2n}{n} = \frac{(2n)(2n-1)\cdots(n+1)}{n!}$$

~~can only have 1 appearance on numerator~~

At most one of $\{(n+1), \ldots, 2n\}$ is divisible by p. Say p^x.

Then $k \leq x$. So $p^k \leq p^x \leq 2n$

$\psi(x) = \sum_{n \leq x} \Lambda(n)$, $\Lambda(n) = \begin{cases} \log p, & n = p^k \\ 0, & \text{o.w.} \end{cases}$

Note: $\lfloor \log_p x \rfloor$ is largest power of p s.t. $\sim$.

$$\psi(x) = \sum_{p \leq x,\, p \text{ prime}} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p. \checkmark$$

$$\psi(2n) = \sum_{p \leq 2n,\, p \text{ prime}} \left\lfloor \frac{\log 2n}{\log p} \right\rfloor \log p.$$

$N = \binom{2n}{n}$. $p^k \leq 2n$.

~~$\psi(N) = \sum_{p \leq N, p^k \leq N} \lfloor \frac{\log N}{\log p} \rfloor \log p$~~

$$e^{\log p \lfloor \frac{\log 2n}{\log p} \rfloor} = p^{\lfloor \log_p 2n \rfloor}$$

$$\prod_{p \leq 2n} p^{\lfloor \log_p 2n \rfloor} \geq \binom{2n}{n}$$

$$\psi(x) \geq \log \binom{2n}{n}$$

$$\geq \log 2^n$$

$$\geq n \log 2,$$

~~$2^{2^k} \equiv -1 (P)$~~

$m = 2^k$

$P \mid 2^{2^k} + 1.$

$2^{2^k} + 1 \equiv 0 (P)$

$2^{2^k} \equiv -1 (P).$

$2^{P-1} \equiv 1 (P)$

$\left(\frac{2}{P}\right) = \begin{cases} 1, & P \equiv 1 (4) \\ -1, & P \equiv 3 (4) \end{cases}$

$\left(\frac{2}{P}\right) = 1$

$(2^{2^k})^2 \equiv 1 (P).$

$2^{2 \cdot m} \equiv 1 (P)$

$\frac{P-1}{2} + k(P-1) = 2^k = m.$

$2^{\frac{P-1}{2}} \equiv 1 (P)$

2017. P,S1.

$2^{P-1} \equiv 1 (P).$

$2^{2^k} \equiv -1 (P).$

$\Rightarrow P \equiv 1 (m).$

$\Rightarrow \left(\frac{2}{P}\right) = 1 \Rightarrow 2^k = k(P-1) + \left(\frac{P-1}{4}\right).$

$\Rightarrow P \equiv 1 (4m)$

2016. P4, SI

(d) $p, 3p-2$ primes

$$b^{N-1} \equiv 1 \, (N)$$

$$\Leftarrow \quad b^{N-1} \equiv 1 \, (p)$$

$$b^{N-1} \equiv 1 \, (3p-2).$$

$$b^{p-1} \equiv 1 \, (p)$$

$$b^{p(3p-2)-1} \equiv b^{3p-3} = \cancel{b^{3-2} \equiv b(p)} \; 1 \, (p)$$

~~RE~~

$$\cancel{b^{p} \equiv b^{3p-2} = b^{3(p-1)+1} \equiv b}$$

$$\cancel{3p^2-2p \quad 3p(p-1)+(p-1)+1}$$

$$\cancel{b^{p(3p-2)} \equiv b}$$

$$\cancel{b^{p(3p-2)}}$$

$$b^{3p-3} \equiv 1 \, (3p-2)$$

$$b^{p(3p-2)-1} = b^{(3p-3)p+p-1}$$

$$\cancel{\equiv 1} = b^{p-1} \equiv 1 \, (3p-2)$$

$$(3p-3, p-1)$$

$$= p-1$$

So $\frac{1}{3}$ ✓

2017.

P4, 5I, 1G.

$$\prod_{\substack{p \le x \\ p \text{ prime}}} \left(1-\frac{1}{p}\right)^{-1} > \log x \checkmark.$$

$$e^{-\sum \frac{1}{p}}$$

$$e^{-x} = 1 - x + \cdots$$
$$< 1 - x.$$

$$e^{-\sum \frac{1}{p}} < \prod \left(1 - \frac{1}{p}\right)$$
$$< \frac{1}{\log x}.$$

$$\log \log x + c. \checkmark$$

NT: Day 2

BQF

1. 若 $n = x^2 + y^2$. $p \mid n$

$x^2 \equiv -y^2 \ (p)$

$\left(\frac{-1}{p}\right) = 1$

$\Longrightarrow$ if $x, y \not\equiv 0 \ (p)$, then $p \equiv 1 (4)$

if $x, y \equiv 0 \ (p)$, then ~~$p^2 \mid n$~~ p even power $\mid n$

So any $p \equiv 3 (4)$, ~~$p^2 \mid n$~~ even power.

$(\Leftarrow)$ $(a^2+b^2)(c^2+d^2)$

$= (ac-bd)^2 + (ad+bc)^2$ $\quad (a+bi)(c+di) = (ac-bd) + i(ad$

So 若 $\boxed{\text{every } p \equiv 1(4) \text{ expressible, then } \checkmark}$.

Prove later.

2. same discriminant not equivalent:

$\begin{cases} x^2 + 6y^2 \\ 2x^2 + 3y^2 \end{cases}$

equivalent BQF rep same set of integers:

$f(x,y) = ax^2 + bxy + cy^2$ $\quad \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$

$f(\alpha_1 x + \beta_1 y, \alpha_2 x + \beta_2 y)$

~~Equivalent~~:

Unimodular sub: $(X,Y)=(x,y)A$, $A\in SL_2(\mathbb{Z})$.

f, g equivalent if $f(X,Y)=g(x,y)$

for one unimodular sub $(x,y)\mapsto(X,Y)$.

$g(x,y)=f(X,Y)=f((x,y)A)$. ✓

$f(X,Y)=g(x,y)=g((X,Y)A^{-1})$. ✓

---

3. $d \Rightarrow d\equiv 0,1\ (4)$

$d\equiv 0,1\ (4) \Rightarrow d=4k$ or $4k+1$

✓

4: $T_{\pm}$: $(a,\ b\pm 2a,\ a\pm b+c)$ (i)

S: $(c,\ -b,\ a)$ (ii)

5 $-a<b\le a<c$

or $0\le b\le a=c$.

~~6. $|a|\le|b|\le$~~ ~~$|b|\le a\le c$.~~

~~By (i) can reduce b s.t. $|b|\le|a|$.~~

~~By (ii), keep $|b|$ unchanged, swap a, c.~~

~~Then after several (i), if $a>c$, swap.~~

~~so always $|a|\le|c|$.~~

6. If $a>c$: use S, $a\downarrow$, $|b|$ same,

if $a\le c$, $|b|>a$: use $T_\pm$, $|b|\downarrow$,

a unchanged.

Then $a+|b|$ decreased in each step.

In the end get (a,b,c), $a\le c$, $|b|\le a$.

If $a<c$, then ① $b>-a$ ✓

② $b=-a$, $T_+ \to (a,a,c)$, ✓.

If $a=c$, ① (a,b,c) reduced ✓

② $-a<b<0$,

use $S \to (a,-b,a)$ ✓.

7. $|b|\le a\le c$,

~~$|b|\le a$~~

$b^2-4ac=d$

$|b^2-4ac| = |4ac-b^2|$

$= 4ac-b^2$

$\geq 4a^2-a^2$

$= 3a^2 \Rightarrow$ ~

$b^2\equiv d\,(4)$

$\Rightarrow b\equiv d\,(2)$.

Callbach

8. Any $P \equiv 1 (4)$ is a sum of two squares.

$\left(\frac{-1}{P}\right) = 1$, so $x^2 \equiv -1 (P)$.

$x^2+1 = Pk$ ~~$(4m+1)k$~~

~~$(P, 2x, k)$~~

$(2x)^2 - 4Pk = -4$.

$h(P, 2x, k) = -4$

$(P, 2x, k) \sim (1, 0, 1)$. reduced.

$\downarrow$

rep: P. ✓.

---

9. Properly rep. ~~(x, y)~~ $(\alpha, \beta) = 1$. $f(\alpha, \beta)$

---

10. $ax^2+bxy+cy^2$

If $y=0$: a

If $x=0$: c

If $x, y \geq 1$: Wlog $|x| \geq |y|$:

$ax^2+bxy+cy^2 \geq ax^2 - |b||x||y| + cy^2$

$\geq (a-|b|)x^2 + cy^2$.

$\geq a - |b| + c \geq c$.

11. $a, c, a-|b|+c$

So either $ax^2+bxy+cy^2$

or $ax^2-bxy+cy^2$.

But $\downarrow$ not equivalent

So unique.

---

12. $f \sim (n,b,c)$, then ✓

if f properly rep n,

$f(\alpha,\beta)=n$.

~~$a\alpha+b\beta=1$~~ $\quad a\alpha^2+b\alpha\beta+c\beta^2=n$

$t\alpha+s\beta=1$.

$\begin{pmatrix} t & -s \\ \beta & \alpha \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$.

$g(x,y) = f((\alpha x-sy),(\beta x+ty)) = f(X,Y)$

$x^2(a\alpha^2+c\beta^2+b\alpha\beta)+\cdots$

$=nx^2+\cdots$

---

13. $d\equiv 0,1\ (4)$.

n properly rep

If $x^2\equiv d\ (4n)$ soluble, $x^2+4nk=d$.

$(n,x,-k)$ ✓

f n properly rep by f, then $f\sim(n,b,c)$, $d=b^2-4nc$

$b^2\equiv d\ (4n)$ ✓

4. $T_{\pm} = (a, \overset{b \pm 2a}{\cancel{a \pm 2b + c}}, a \pm b + c)$.

$S = (c, -b, a)$

2021. P3. S II.

11 I. $h(d) = \#$ distinct reduced p.d. BQF.

Equivalent: $f(x,y) = g(X, Y)$

$(x, y) \mapsto (X, Y)$ through a unimodular transformation

$m \in \mathbb{Z}^+$, f BQF.

f properly rep $m \Rightarrow$ $\exists$ (α, β) $t\alpha + \beta s = 1$.

$a\alpha^2 + b\alpha\beta + c\beta^2 = m$

$\sim$

$\sim (m, b, c)$.

$d < 0$ m properly rep by d, iff $d \equiv x^2 (4m)$ soluable ✓.

Fix $A \geq 2$,

claim: n^2+n+A composite for some n s.t. $0 \leq n \leq A-2$.

$\Leftrightarrow$ $d = 1-4A$ is a square mod $4p$ for some $p < A$.

proof: ~~If $d = 1-4A \equiv b^2\ (4p)$ for some $p<A$~~

~~Then~~

($\Rightarrow$) If $p \mid A+n^2+n$ for some $0 \leq n \leq A-2$, then

$$A+n^2+n = pk.$$

$$4A+(2n)^2+4n = 4pk.$$

$$(2n^2)+4n \equiv -4A\ (4p)$$

$$1-4A \equiv (2n+1)^2\ (4p).$$

so $d = 1-4A$ is a square mod $4p$.

($\Leftarrow$) If $d = 1-4A$ is a square mod $4p$ for some $p < A$.

$1-4A \equiv (2b+1)^2 (4p)$ as by consider mod 4 square must be odd.

So $4A+4b^2+4b \equiv 0\ (4p)$.

$$A+b^2+b \equiv 0\ (p).$$

$$p \mid A+b^2+b.$$

Also, ~~can choose b s.t.~~

since $p<A$,

$2b+1$ ~~$\in \mathbb{Z}/\mathbb{Z}_p$~~ is under mod p,

so can choose b s.t. $0 \le 2b+1 \le p$,

$b \le p-1 \le A-2$.

~~Thus~~ So true.

Thus iff n^2+n+A prime $\forall n=0,1,\dots,A-2$

$\Leftrightarrow$ $d=1-4A$ not a square mod $4p$. $\forall p<A$.

$\Leftrightarrow$ p not properly rep by BQF ~~$\forall$~~ of ~~...~~ $d=1-4A$

$\forall p<A$.

~~If (a,b,c), $b^2-4ac=1-4A$~~

~~$(2k+1)^2-4ac=1-4A$.~~

~~$k^2+k+A=ac$.~~

$(\Rightarrow)$ ~~Since $(1,1,A)$ reduced~~, $d(1,1,A)=1-4A$.

Least three pos int. properly rep are $1, A$,

$(\Leftarrow)$ $(1,-1,A)$ reduced.

$d(1,-1,A)=1-4A$.

Least integers are $1, A$.

(⇐) If (a,b,c) reduced.

$b^2-4ac=1-4A$.

$b=2k+1$.

$k^2+k+A=ac$.

Then ① if $0\le k\le A-2$, k^2+k+A is prime

so $(a,b,c)=(1,\cancel{2k+1}\ \pm(2k+1),k^2+k+A)$.

~~If $k\neq 0$, then~~

Reduced $\Rightarrow k=0$.

so must be $(1,-1,A)$.

If $k\geq A-1$: $|b|^2=(2k+1)^2$

$\leq|a||c|=k^2+k+A$.

#.

So ✓.

(⇒) If $h(1-4A)=1$, then

must equivalent to $(1,-1,A)$.

~~which~~ Least integers $1,A$.

If n^2+n+A not prime, $n^2+n+A=ac$,

$a>1, c>1$.

~~Say then~~

Then a,c rep by $(1,-1,A)$, #.

NT Day 3.

Contimed Fractions.

1. CFE terminates iff $\theta \in \mathbb{Q}$:

$(\Rightarrow)$ ✓

$(\Leftarrow)$ Numerators in the minimal fraction of θ_i is strictly decreasing with i, so must hit 1 eventually.

$$\theta = [a_0, a_1, \ldots, a_n, \theta_n]$$
$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{\theta_n}}}}.$$

---

2. $p_{-1} = 1$ $p_0 = a_0$ $p_1 = a_0a_1+1$ ... $p_n = a_n p_{n-1} + p_{n-2}$

$q_{-1} = 0$ $q_0 = 1$ $q_1 = a_1$ ... $q_n = a_n q_{n-1} + q_{n-2}$

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \cancel{\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}}$$
$$\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}$$

3. $p_n q_{n-1} - q_n p_{n-1}$

$= \cancel{(\ldots q_n a_n\, a_n q_{n-1})}$

$= (a_n p_{n-1} + p_{n-2})\, q_{n-1} - (a_n q_{n-1} + q_{n-2})\, p_{n-1}$

$= -[p_{n-1} q_{n-2} - p_{n-2} q_{n-1}]$

4. $\alpha = \dfrac{p_n \beta + p_{n-1}}{q_n \beta + q_{n-1}}$: Induction

$\beta' = a_n + \dfrac{1}{\beta}$.

$$\alpha = \frac{p_{n-1}\beta' + p_{n-2}}{q_{n-1}\beta' + q_{n-2}} = \frac{p_{n-1}(a_n + \frac{1}{\beta}) + p_{n-2}}{q_{n-1}(a_n + \frac{1}{\beta}) + q_{n-2}} = \sim.$$

$$\alpha - \frac{p_n}{q_n} = \frac{(p_n\beta + p_{n-1})q_n - p_n(q_n\beta + q_{n-1})}{(q_n\beta + q_{n-1})\, q_n} = \frac{(-1)^n}{q_n(q_n\beta + q_{n-1})}$$

5. $$\left|\theta - \frac{p_n}{q_n}\right| = \left|\frac{-1}{q_n(q_n\beta + q_{n-1})}\right| < \left|\frac{1}{q_n(q_n a_n + q_{n-1})}\right| = \frac{1}{q_n q_{n+1}}$$

6. $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$: Induction.

7. $1 \leq q < q_{n+1} \Rightarrow |q\theta - p| \geq |q_n\theta - p_n|$:

$1 \le q < q_{n+1} \Rightarrow |q\theta - p| \geq |q_n\theta - p_n|$:

~~$q_n u + p_n v = 1$~~

$$\begin{cases} p_n u + p_{n+1} v = p \\ q_n u + q_{n+1} v = q. \end{cases}$$

$$|q\theta - p| = \left|(q_n u + q_{n+1} v)\theta - (p_n u + p_{n+1} v)\right|$$
$$= \left| u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})\right|$$

$1 \le q < q_{n+1} \Rightarrow u, v$ opposite sign.

If $v = 0$, then ~

$u \neq 0$.

Then $| \quad | \geq | \quad | + | \quad |$ ~ .

8. $7 \Rightarrow 8$.

9. If $\left|\theta - \frac{p_n}{q_n}\right| \geq \left|\frac{1}{2q_n^2}\right|$

$\left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| \geq \left|\frac{1}{2q_{n+1}^2}\right|$, then

$$\left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}$$

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right|, \qquad \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} = \frac{q_n^2 + q_{n+1}^2}{2q_n^2 q_{n+1}^2}$$

$\Leftrightarrow$ ~~$q_n^2 + q_{n+1}^2 \geq 2q_n q_{n+1}$~~ $q_n^2 + q_{n+1}^2 \le 2q_n q_{n+1}$ #.

10. $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$.

~~Say $1 \le q < q_{n+1}$, then $|q_n\theta - p_n| \le |q\theta - p| < \frac{1}{2q} \le \frac{1}{2q_n}$.~~

$q_n \le q < q_{n+1}$. If $\frac{p}{q} \ne \frac{p_n}{q_n}$, then

$$\frac{1}{qq_n} \le \left|\frac{p}{q} - \frac{p_n}{q_n}\right| \le \left|\theta - \frac{p}{q}\right| + \left|\theta - \frac{p_n}{q_n}\right|$$

$$= \frac{1}{q}|\theta q - p| + \frac{1}{q_n}|q_n\theta - p_n|$$

$$\cancel{\le \left(\frac{1}{q} + \frac{1}{q_n}\right)\left(|q_n\theta - p_n|\right)}$$

$$\le \left(\frac{1}{q} + \frac{1}{q_n}\right)\left(|\theta q - p|\right)$$

$$< \frac{1}{2q^2} + \frac{1}{2qq_n}$$

$$\frac{1}{qq_n} < \frac{1}{2q^2} + \frac{1}{2qq_n} \Rightarrow q < q_n. \quad \#$$

11. Periodic $\Rightarrow$ quadratic irrational:

$\theta = [a_0, \dots, a_n, \phi] = [a_0, \dots, a_n, \overline{a_{n+1}, \dots, a_m}]$.

Then $\theta = \frac{p_n\phi + p_{n-1}}{q_n\phi + q_{n-1}}$

Note: $\phi = [\overline{a_{n+1}, \dots a_m}] = [a_{n+1}, \dots, a_m, \phi]$

so $\frac{p_k\phi + p_{k-1}}{q_k\phi + q_{k-1}} = \phi$.

$\Rightarrow$ a quadratic irrational.

$\Rightarrow$ ~

12. If $d \in \mathbb{N}$ not a square, then
$x^2-dy^2=1$ has a sol $(x,y)\in\mathbb{Z}^2$ with $xy\neq 0$.

Proof: Let $\theta=\sqrt{d}=[a_0,\overline{a_1,\dots,a_n}]$.

$$=[a_0,a_1,\dots,a_n,\theta_{n+1}],$$

with $\theta_1=\theta_{n+1}=[\overline{a_1,\dots,a_n}]$.

Assume n even [if not, replace n by $2n$].

Note $\theta=a_0+\frac{1}{\theta_1}$, so $\frac{1}{\theta_1}=\theta-a_0$.

$$\sqrt{d}=\frac{p_n\theta_1+p_{n-1}}{q_n\theta_1+q_{n-1}}=\frac{p_n+p_{n-1}(\sqrt{d}-a_0)}{q_n+q_{n-1}(\sqrt{d}-a_0)}$$

$$q_{n-1}d+(q_n-q_{n-1}a_0)\sqrt{d}=p_n-a_0p_{n-1}+p_{n-1}\sqrt{d}.$$

$$\Rightarrow \quad p_{n-1}=q_n-q_{n-1}a_0$$
$$q_{n-1}d=p_n-a_0p_{n-1}.$$

$$\Rightarrow \quad p_{n-1}^2-q_{n-1}^2d=(-1)^n=1 \checkmark.$$

NT. 2022.

P4, SI, II

$$\sqrt{29} = 5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{10 + \boxed{\text{repeat}}}}}}} = [5, \overline{2,1,1,2,10}]$$

$$\frac{1}{\sqrt{29}-5} = \frac{\sqrt{29}+5}{4} = 2 + \frac{\sqrt{29}-3}{4}$$

$$\frac{4}{\sqrt{29}-3} = \frac{4(\sqrt{29}+3)}{20} = \frac{\sqrt{29}+3}{5} = 1 + \frac{\sqrt{29}-2}{5}$$

$$\frac{5}{\sqrt{29}-2} = \frac{5(\sqrt{29}+2)}{25} = \frac{\sqrt{29}+2}{5} = 1 + \frac{\sqrt{29}-3}{5}$$

$$\frac{5}{\sqrt{29}-3} = \frac{5(\sqrt{29}+3)}{20} = \frac{\sqrt{29}+3}{4} = 2 + \frac{\sqrt{29}-5}{4}.$$

$$\frac{4}{\sqrt{29}-5} = \frac{4(\sqrt{29}+5)}{4} = \sqrt{29}+5 = 10 + (\sqrt{29}-5)$$

	~~0~~	~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~
~~a_i~~	~~5~~		~~2~~	~~1~~	~~1~~	~~2~~	~~10~~
~~p_i~~	~~1~~	~~5~~					
~~q_i~~	~~0~~	~~1~~					

	0	1	2	3	4	5
a_i	5	2	1	1	2	10
p_i	5	11	16	27	70	727
q_i	1	2	3	5	13	135

$\cancel{727^2 - 135^2 \cdot 29}$

$70^2 - 13^2 \cdot 29 = -1$

If $\left|\theta - \frac{p}{q}\right| < \left|\theta - \frac{p_n}{q_n}\right|$

$p_n u + p_{n+1} v = p$

$q_n u + q_{n+1} v = q$.

$\therefore \quad |q\theta - p| \geq |q_n\theta - p_n|$.

If $q < q_{n+1}$.

If $q < q_n$: $q\left|\theta - \frac{p}{q}\right| < q\left|\theta - \frac{p_n}{q_n}\right|$

$\Rightarrow |q\theta - p| < q_n\left|\theta - \frac{p_n}{q_n}\right|$

$= |q_n\theta - p_n|$,

找.

So ~.

NT. 2017.

P3, SII, 10Q.

$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_m}]$

(a) ✓

(b) $\theta_n = \frac{\sqrt{d} + r_n}{s_n}$

$$\sqrt{d} = \frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}}.$$

$$= \frac{\frac{(\sqrt{d} + r_n)}{s_n} p_{n-1} + p_{n-2}}{\frac{\sqrt{d} + r_n}{s_n} q_{n-1} + q_{n-2}}$$

$$= \frac{(\sqrt{d} + r_n) p_{n-1} + p_{n-2} s_n}{(\sqrt{d} + r_n) q_{n-1} + q_{n-2} s_n}.$$

$$d q_{n-1} + \sqrt{d}[r_n q_{n-1} + q_{n-2} s_n] = \sqrt{d}\, p_{n-1} + (r_n p_{n-1} + p_{n-2} s_n)$$

So; $r_n q_{n-1} + q_{n-2} s_n = p_{n-1}$

$d q_{n-1} = r_n p_{n-1} + p_{n-2} s_n$.

$$\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} r_n \\ s_n \end{pmatrix} = \begin{pmatrix} d q_{n-1} \\ p_{n-1} \end{pmatrix}.$$

$\Rightarrow \begin{pmatrix} r_n \\ s_n \end{pmatrix} = \sim$. are integers.

(c) Use $\theta_1 = \theta_{m+1} = [\overline{a_1, a_2, \ldots, a_m}]$, find $p_{n-1}, q_{n-1} d$

$= \sim \Rightarrow p_{n-1}^2 - q_{n-1}^2 d$

NT. Day 4

Distribution of Primes

1. $\pi(x) \geq \frac{\log x}{2\log 2}$: Write $x = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$p_k < \sqrt{x}$.

$\alpha_i < \frac{\log x}{\log 2}$.

Total choice

Let $p_1, \ldots, p_r$ be primes up to x.

$n = k^2 \prod_{i=1}^{r} p_i^{\alpha_i}$, $\alpha_i \in \{0,1\}$, $1 \leq k \leq \sqrt{x}$.

k: $\sqrt{x}$ choices

α_i: 2^r choices

$x \leq \sqrt{x}\, 2^r = \sqrt{x}\, 2^{\pi(x)} \Rightarrow 2^{\pi(x)} \geq \sqrt{x}$

$\Rightarrow \pi(x) \geq \frac{\log_2 x}{2}$.

2. $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod \left(1 - \frac{1}{p^s}\right)^{-1}$.

3. $\mu(n) = \begin{cases} (-1)^k, & n \text{ product of } k \text{ distinct primes.} \\ 0, & n \text{ square-free} \end{cases}$

$\mu(n)$ is multiplicative:

$\Rightarrow \cancel{\sum_{f|d} \mu(n)} = \sum_{e|d} \mu(e)$ is multiplicative

$v(n)$

$= \mathbb{1}[n=1]$.

4. $g(n) = \sum_{d|n} f(d)$

$\Leftrightarrow f(n) = \sum_{e|n} \mu(e)\, g\left(\frac{n}{e}\right)$

prof: $(\Rightarrow)$ $\sum_{e|n} \mu(e) \sum_{d|\frac{n}{e}} f(d)$

$= \sum_{d|n} f(d) \underbrace{\sum_{e|\frac{n}{d}} \cancel{\mu(e)}\, \mu(e)}_{= \mathbb{1}[\frac{n}{d}=1]}$

$= f(n)$

$(\Leftarrow)$ $\sum_{d|n} f(d)$

$= \sum_{d|n} \sum_{e|d} \mu(e)\, g\left(\frac{d}{e}\right)$

$= \sum_{d|n} g(d) \sum_{e|\frac{n}{d}} \mu(e)$

$= f(n)$.

5. $\Lambda(n) = \begin{cases} \log p, & n = p^k \\ 0, & \text{o.w.} \end{cases}$

$sp^{-(s+1)}$

$\cancel{\frac{\zeta'(s)}{\zeta(s)}}$ $\log \zeta(s) = -\sum_p \log(1-p^{-s})$

$\Rightarrow \frac{\zeta'(s)}{\zeta(s)} = \cancel{-\frac{d}{ds} - \sum \frac{p^{-s}\log p}{1-p^{-s}}}$

$= -\sum_p \frac{p^{-s}\log p}{1-p^{-s}} = -\sum_p (\log p)(p^{-s}) \sum_{k=0}^{\infty} p^{-ks}$

$= -\sum \log p \sum^{\infty} p^{-js}$

$= -\sum \frac{\Lambda(n)}{n^s}$ $j=1$

Legendre: $x>1$, $P=\prod_{p \text{ prime} \le \sqrt{x}} p$

$$\pi(x)-\pi(\sqrt{x})+1 = \sum_{d|P} \mu(d)\left[\frac{x}{d}\right].$$

$|\{1\le n\le x : (n,P)=1\}|$

$$= \sum_{1\le n\le x} \mathbb{1}[(n,P)=1]$$

$$= \sum_{1\le n\le x} \sum_{d|(n,P)} \mu(d)$$

$$= \sum_{d|P} \mu(d) \sum_{\substack{1\le n\le x,\\ d|n}} 1 = \sum_{d|P} \mu(d)\left[\frac{x}{d}\right].$$

6. Let N be odd & composite.

$\exists\, b$ s.t. $b^{\frac{N-1}{2}} \not\equiv \left(\frac{b}{N}\right) (N)$.

Proof: ① If N ~~not~~ is square-free, then $N=p_1p_2\cdots p_k$.

$\rightarrow$ u is N-QR of p_1

Let $b\equiv u\ (p_1)$

$b\equiv 1\ (p_2)$ Then $\left(\frac{b}{N}\right)=-1$.

$b\equiv 1\ (p_3)$

$\vdots$

$b\equiv 1\ (p_k)$

~~$b^{\frac{p_2\cdots p_k}{2}-1} = \left(\frac{b}{p_2\cdots p_k}\right)$~~

~~$b^{\frac{p_2\cdots p_k-1}{2}}$~~

$b\equiv 1\ (\text{mod } p_2\cdots p_k)$

~~$b^{\frac{N-1}{2}} \not\equiv$~~ ~~$\Rightarrow b^{\frac{N-1}{2}} (\text{mod } p$~~

$\Rightarrow b^{\frac{N-1}{2}} \equiv 1\ (\text{mod } p_2\cdots p_k)$

$\not\equiv -1$

So $b^{\frac{N-1}{2}} \not\equiv -1\ (\text{mod } p_1p_2\cdots p_k)$

② If $p^2 | N$,

$(1+p)^{N-1} \equiv 1+(N-1)p \not\equiv 1\ (p^2)$.

Exist ~~Take~~ $b \equiv 1+p\ (p^2)$, $(b,N)=1$ by CRT.

$b^{N-1} \not\equiv 1\ (p^2)$, so $b^{\frac{N-1}{2}} \not\equiv \pm 1$. So ~.

7. Strong pseudoprime: N to b:

$N-1 = 2^s \cdot t$, t odd.

$b^{t \cdot 2^r} \equiv -1\ (N)$ for some $0 \le r < s$

or $b^{t \cdot 2^r} \equiv 1\ (N)$ for all $0 \le r \le s$

i.e. $b^t \equiv 1\ (N)$.

2022.

P1, S I, 1 I.

$\phi(n) = |\{x : (x, n) = 1\}|$

$\mu(d) = \begin{cases} (-1)^k, & d = p_1 p_2 \cdots p_k \\ 0, & d \text{ is not square free} \end{cases}$

~~$\mu(d)$~~

$\sum_{d|n} \frac{\mu(d)}{d}$ $\quad \frac{\mu(d)}{d}$ is multiplicative

$\Rightarrow \sum_{d|n} \frac{\mu(d)}{d}$ is multiplicative.

$$\frac{\phi(p)}{p} = \frac{\mu(p)}{p} + \frac{\mu(1)}{1}$$

$$\frac{p-1}{p} \qquad 1 - \frac{1}{p}.$$

P4, S V, 1 I.

(a) $\left(\frac{2}{p}\right) = [2, 4, \cdots, 2 \cdot \frac{p-1}{2}]$

$\frac{p-1}{2}$ $\quad x^2 \equiv 2 \ (p)$ solvable $\Leftrightarrow p \equiv \pm 1 \ (8)$

(b)(i) $\pi_7(x) \to \infty$ as $x \to \infty$;

$p \equiv 7 \ (8)$

n^2-2 for n in a suitable range,

$$n^2-2 = \overset{3}{\cancel{\alpha}}\, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

$0, 1, 2.$

$\downarrow \quad \downarrow$

$\leq \sqrt{n}$

$$n^{\frac{2}{3}} \cdot 3^{\pi_1(n^2)+\pi_7(n^2)} \geq n$$

$$\pi_1(n^2)+\pi_7(n^2) \geq \log_3 n^{\frac{1}{3}}$$

$$= \frac{1}{3}\log_3 n.$$

$$\Rightarrow \sim \geq \frac{\log x}{6\log 3}.$$

P4, SII, 11G. NT 2018.

(a) ✓

(b) Fermat : $b^{N-1} \equiv 1 \ (N)$.

Carmichael : $b^{N-1} \equiv 1 \ (N)$

$\forall b$ s.t. $(b, N) = 1$.

Claim: ~~Every~~ Carm number is square-free.

Proof. ~~PSUF~~ ~~PSF~~

If $p^2 | N$, then:

$b^{N-1} \equiv 1 \ (N)$

$\Rightarrow b^{N-1} \equiv 1 \ (p^2)$

~~But (1+p)~~

$$\pi(x) - \pi(\sqrt{x}) + 1$$

$$= \left|\{1 \le n \le x : (n, P) = 1\}\right|$$

$$= \sum_{d \mid P} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor, \qquad P = \prod_{p \text{ primes} \le \sqrt{x}} p.$$

primes $\le \sqrt{42}$: 2, 3, 5, ~~6~~.

$$\pi(42) - \pi(\sqrt{42}) + 1$$

$$= 42 - \left[\left\lfloor \frac{42}{2} \right\rfloor + \left\lfloor \frac{42}{3} \right\rfloor + \left\lfloor \frac{42}{5} \right\rfloor - \left\lfloor \frac{42}{6} \right\rfloor - \left\lfloor \frac{42}{10} \right\rfloor - \left\lfloor \frac{42}{15} \right\rfloor + \left\lfloor \frac{42}{30} \right\rfloor \right]$$

$$= 42 - 21 - 14 - 8 + 7 + 4 + 2 - 1$$

$$= 54 - 35 - 8$$

$$= 19 - 8 = 11.$$

$$\pi(42) = 11 + 3 - 1 = 13.$$

2 3 5 7
11 13 17 19
23 29 31 37
41
$\Rightarrow$ 13

$$\cancel{\left|\{1\le n\le x : (n,p)=1\}\right|}$$

$$= \cancel{[illegible] \sum_{1\le n\le x} \mu_{(n,p)}}$$

$$\cancel{\sum_{1\le n\le x} \sum_{d\mid(n,p)} \mu((n,p))}$$

$$\cancel{= \sum_{1\le n\le x} \sum}$$

$$\left|\{1\le n\le x : (n,p)=1\}\right|$$

$$= \sum_{1\le n\le x} \mathbb{1}_{(n,p)=1}$$

$$= \sum_{1\le n\le x} \sum_{d\mid(n,p)} \mu(d)$$

$$= \sum_{d\mid p} \mu(d) \sum_{1\le n\le x,\, d\mid n} 1$$

$$= \sum_{d\mid p} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor.$$