Chinese remainder theorem

$$\text{Let} \quad \begin{matrix} n_1 \dots n_r \in \mathbb{N} \\ a_1 \dots a_r \in \mathbb{Z} \end{matrix} \Big/ \gcd(n_i, n_j) = 1 \forall i \neq j$$

then the system $\begin{cases} x & \equiv & a_1[n_1] \\ x & \equiv & a_2[n_2] \\ \vdots & \vdots & \vdots \\ x & \equiv & a_r[n_r] \end{cases}$
has a simultaneous solution which is unique modulo $n_1 \cdot n_2 \dots n_r$

$$\Rightarrow f(x) \equiv 0[n] \text{ with } n = p_1^{k_1} \dots p_r^{k_r} \qquad \begin{cases} f(x) & \equiv & 0[p_1^{k_1}] \\ & \vdots & \\ f(x) & \equiv & 0[p_r^{k_r}] \end{cases}$$

Set

$$n = n_1 \dots n_r$$

And

$$N_k = \frac{n}{n_k} = n_1 n_2 \dots n_{k-1} n_{k+1} \dots n_r$$

Then, $N_k x_k \equiv 1[n_k]$

$$N_k x_k + n_k y_k = 1, \text{exists because } \gcd(N_k, n_k) = 1$$

And if we set $\bar{x} \equiv \sum_{k=1}^{r} a_k N_k x_k \equiv a_k[n_k]$, then $\bar{x}$ is a simultaneous solution.

Fermat's theorem

Let p be a prime, $a \in \mathbb{Z}/ \quad p \nmid a$. Then,

$$a^{p-1} \equiv 1[p]$$

Wilson's theorem

If p is a prime, then $(p-1)! \equiv -1[p]$

Number and sum of divisors

$$\begin{matrix} \tau(n) & = \sum_{d|n} 1, \text{ the number of positive divisors of n.} \\ \sigma(n) & = \sum_{d|n} d, \text{ the sum of the positive divisors of n.} \end{matrix}$$

Theorem. *Let $n > 1$ with $n = p_1^{k_1} \cdots p_r^{k_r}$. Then*

1. $\tau(n) = (k_1 + 1) \cdots (k_r + 1)$
2. $\sigma(n) = (\frac{p_1^{k_1+1}-1}{p_1-1}) \dots (\frac{p_r^{k_r+1}-1}{p_r-1})$

Theorem. *Let f be a multiplicative number theoretic function and define $F(n)$ by:*

$$F(n) = \sum_{d|n} f(d), \qquad n \geq 1$$

Then F is also a multiplicative number theoretic function.

Corollary : σ and τ are multiplicative

Möbius function μ

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } \exists p \text{ prime such that } p^2 \mid n \\ (-1)^r & \text{if } n = p_1 p_2 \dots p_r, \text{ with distinct primes.} \end{cases}$$

Theorem. *μ is multiplicative.*

Theorem. *For $n \geq 1$,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Möbius inversion formula

Let F and f be connected by

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

Then

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$$

Theorem. *Let f, F be connected by:*

$$F(n) = \sum_{d|n} f(d)$$

If F is multiplicative, then f is multiplicative.

Euler's φ function

$$\varphi(n) = \mid \{a \in \mathbb{Z} : 1 \leq a \leq n, \quad \gcd(a, n) = 1\} \mid$$

Theorem. *For p prime, $k > 0$:*

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$$

Theorem. *φ is multiplicative.*

Lemma : Let $n > 1$, and $\gcd(a, n) = 1$. If

$$a_1, \ldots, a_{\varphi(n)} \in [1, n)$$

are the positive integers which are relatively prime to n, then

$$aa_1, \ldots, aa_{\varphi(n)}$$

are congruent to $a_1, \ldots, a_{\varphi(n)}$ modulo n in some order.

Euler's theorem

Let $n > 1$ and $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1[n]$$

Lemma : For $n \geq 1$, let

$$S_d = \{m : \quad 1 \leq m \leq n, \quad \gcd(m, n) = d\}.$$

Then

$$\{1, 2, \ldots, n\} = \bigcup_{d|n} S_d$$

and the union is disjoint.

Gauss' theorem

For $n \geq 1$,

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

Theorem. *For $n \geq 1$,*

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

Theorem. *Let $\mathrm{ord}_n(a) = k$, then:*

$$\begin{array}{l} a^i \equiv a^j[n] \\ \iff i = j[k] \end{array}$$

Theorem. *Let $\mathrm{ord}_n(a) = k, h > 0$*
Then a^h has order $\mathrm{ord}_n(a^h) = \frac{k}{\gcd(h,k)}$

Lagrange's theorem: Let p be a prime, and f such that:

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \quad a_i \in \mathbb{Z}, \quad a_n \not\equiv 0[p]$$

Then $f(x) \equiv 0[p]$ has at most n incongruent solutions. **Corollary:** For p prime, $d \mid p-1$:

$$x^d - 1 \equiv 0[p]$$

has exactly d incongruent solutions.

Theorem. *Let p be a prime, $d \mid p-1$, then there are exactly $\varphi(d)$ incongruent integers of order d modulo p.*

Corollary: A prime p has exactly $\varphi(p-1)$ primitive roots.
Application: $p \equiv 1[4] \Rightarrow x^2 \equiv -1[p]$ has a solution.
Take $d = 4$ in the theorem: $4 \mid p-1$
Then there exists an a of order 4 modulo p.

$$p \mid (a^4 - 1) = (a^2 - 1)(a^2 + 1)$$

$$p \mid a^2 - 1 \text{ or } \mid a^2 + 1$$

$$\Rightarrow \left.\begin{array}{l} a^2 \equiv 1[p] \\ a^2 \equiv -1[p] \end{array}\right\} x = a \text{ is a solution to } x^2 \equiv -1[p]$$

Lemma: p an odd prime, there is a primitive element $r[p]$ such that:

$$r^{p-1} \not\equiv 1[p^2]$$

Theorem. *$k \geq 1$, $\forall p$ odd prime, $\exists r[p^k]$ a primitive root.*

Definition. *For $\gcd(a, n) = 1$, the **index** of a in the base r is the smallest positive integer h such that:*

$$a \equiv r^h[n]$$

$$ind_r(a) = h$$

If $a \equiv b[n]$ then $ind(a) = ind(b)$

Theorem. *n, r as above.*

a) $ind_r(a, b) \equiv ind_r(a) + ind_r(b)[\varphi(n)]$

b) $ind_r(a^k) \equiv k \cdot ind_r(a)[\varphi(n)]$

c) $ind_r(1) \equiv 0$

d) $ind_r(r) \equiv 1[\varphi(n)]$

Euler's criterion: Let p be an odd prime, and $p \nmid a$.
Then a is a quadric residue iff:

$$a^{\frac{p-1}{2}} \equiv 1[p]$$

Theorem. *p an odd prime, $p \nmid a$, $p \nmid b$. Then:*

a) $a \equiv b[p] \Rightarrow (a/p) = (b/p)$

b) $(a^2/p) = 1$

c) $(a/p) \equiv a^{\frac{p-1}{2}}[p]$

d) $(ab/p) \equiv (a/p)(b/p)$

e) $(1/p) = 1 \qquad (-1/p) = (-1)^{\frac{p-1}{2}}$

Corollary:

$$(-1/p) = \begin{cases} 1 \\ -1 \end{cases} \iff \begin{array}{l} p \equiv 1[4] \\ p \equiv 3[4] \end{array}$$

Theorem. *There are infinitely many primes of the form $4k+1$*

Proof. : Assume $p_1 \dots p_n$ are all the primes $\equiv 1[4]$, and set:

$$N = (2p_1 p_2 \dots p_n)^2 + 1$$

Let p be a factor in N, then p is odd since N is odd.

$$\begin{array}{l} p \mid N,\ N \equiv 0[p] \\ (2p_1 p_2 \dots p_n)^2 + 1 \equiv 0[p] \\ \Rightarrow (2p_1 \dots p_n)^2 \equiv -1[p] \\ \Rightarrow (-1/p) = 1 \\ \Rightarrow p \equiv 1[4] \\ \Rightarrow p \mid N - (2p_1 \dots p_n) = 1\text{: absurd!} \end{array}$$

Hence there exists infinitely many primes $\equiv 1[4]$. □

Gauss's lemma: p an odd prime, $p \nmid a$
Let n denote the number of elements in

$$S = \{a, 2a, \dots, (\tfrac{p-1}{2})a\}$$

whose remainders [p] lie in $(\frac{p}{2}, p)$, then:

$$(a/p) = (-1)^n$$

Theorem. *p an odd prime, then:*

$$(2/p) = \begin{cases} 1 \text{ if } p \equiv \pm 1[8] \\ -1 \text{ if } p \equiv \pm 3[8] \end{cases}$$

Corollary: $(2/p) = (-1)^{\frac{p^2-1}{8}}$

Theorem. *p an odd prime.*

$$\sum_{a=1}^{p-1}(a/p) = 0$$

i.e. there are exactly $\frac{p-1}{2}$ quadric residues and $\frac{p-1}{2}$ quadric non residues $[p]$.

Gauss's quadratic reciprocity theorem:
$p \neq q$ two odd primes, then:

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

The exact proof is in the book. **Corollary:** $p \neq q$ two odd primes, then

$$(p/q)(q/p) = \begin{cases} 1 \text{ if } p \text{ or } q \equiv 1[4] \\ -1 \text{ if } p \text{ or } q \equiv 3[4] \end{cases}$$

Corollary: $p \neq q$ two odd primes, then

$$(p/q) = \begin{cases} (q/p) \text{ if } p \text{ or } q \equiv 1[4] \\ -(q/p) \text{ if } p \text{ or } q \equiv 3[4] \end{cases}$$

Theorem. *If $p \neq 3$ is an odd prime, then*

$$(3/p) = \begin{cases} 1 if p \equiv \pm 1[12] \\ -1 if p \equiv \pm 5[12] \end{cases}$$

Lemma:

$$\text{If } \begin{cases} m = a^2 + b^2 \\ n = c^2 + d^2 \end{cases} \Rightarrow mn \text{ is also a sum of two squares.}$$

Thue's Lemma: p a prime, $a \in \mathbb{Z}$, $p \nmid a$
Then $ax \equiv y[p]$ has a solution $x_0, y_0 \in \mathbb{Z}/$

$$0 < |x_0| < \sqrt{p}, \qquad 0 < |y_0| < \sqrt{p}$$

Fermat's theorem: An odd prime p is a sum of 2 squares iff $p \equiv 1[4]$.
Proposition: p a prime of the form $4k+1$ can be represented uniquely as a sum of two squares.

Theorem. *Let $n \in \mathbb{N}$, $n = N^2 m$, with m square free.*
Then $n = a^2 + b^2 \iff m$ contains no prime factor of the form $4k+3$

Theorem. $\gcd(u_n, u_{n+1}) = 1 \qquad \forall n \geq 1$

Proposition: for $m \geq 2$, $n \geq 1$:

$$u_{m+n} = u_{m-1}u_n + u_m u_{n+1}$$

Theorem. *For $m \geq 1$, $n \geq 1$*

$$u_m \mid u_{mn}$$

Theorem. *The* gcd *of two Fibonacci numbers is a Fibonacci number:*

$$\gcd(u_m, u_n) = u_{\gcd(m,n)}$$

Lemma: Let $m = qn + r$, with $m, n, q, r \geq 1$, then:

$$\gcd(u_m, u_n) = \gcd(u_r, u_n)$$

Example:

$$\begin{array}{l|l} \frac{a}{b} = \frac{43}{13} & \frac{43}{13} = 3 + \frac{4}{13} = 3 + \frac{1}{\frac{13}{4}} \\ 43 = 3 \cdot 13 + 4 & \frac{13}{4} = 3 + \frac{1}{4} = 3 + \frac{1}{4}1 \\ 13 = 3 \cdot 4 + 1 & \frac{4}{1} = 4 \\ 4 = 4 \cdot 1 & \end{array}$$

$$\Rightarrow \frac{43}{13} = 3 + \frac{1}{3 + \frac{1}{4}}$$

$$\Rightarrow \frac{13}{43} = 0 + \frac{1}{3 + \frac{1}{3 + \frac{1}{4}}}$$

Notation: $[a_0; a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\vdots \quad \vdots \quad \vdots \quad a_{n-1} + \frac{1}{a_n}}}$

$$\frac{13}{43} = [0; 3, 3, 4]$$

Definition. *$C_k = [a_0; a_1, a_2, \ldots, a_k]_{1 \leq k \leq n}$; is called the k^{th} convergent to $[a_0; a_1, \ldots, a_k, \ldots, a_n]$.*

Example:

$$\left.\begin{array}{l} [0; 3, 3, 4] \\ C_0 = 0 \\ C_1 = 0 + \frac{1}{3} = \frac{1}{3} \\ C_2 = 0 + \frac{1}{3 + \frac{1}{3}} = \frac{3}{10} \\ C_3 = 0 + \frac{1}{3 + \frac{1}{3 + \frac{1}{4}}} = \frac{13}{43} \end{array}\right\} C_k = \frac{p_k}{q_k}, \text{ with } \left[\begin{array}{ll} p_0 = a_0 & q_0 = 1 \\ p_1 = a_1 a_0 + 1 & q_1 = a_1 \\ p_k = a_k p_{k-1} & q_k = a_k q_{k-1} + q_{k-2} \end{array}\right]$$

Theorem. *The k^{th} convergent $C_k = \frac{p_k}{q_k}$ with p_k, q_k given by recursion.*

Convention:

$$\left\{\begin{array}{ll} p_{-2} = 0 & q_{-2} = 1 \\ p_{-1} = 1 & q_{-1} = 0 \end{array}\right. \quad \left(\begin{array}{c|cc|c|c|c|c} k & -2 & -1 & 0 & 1 & 2 & 3 \\ \hline a_k & . & . & 0 & 3 & 3 & 4 \\ p_k & 0 & 1 & 0 & 1 & 3 & 13 \\ q_k & 1 & 0 & 1 & 3 & 10 & 43 \\ C_k & . & . & 0 & \frac{1}{3} & \frac{3}{10} & \frac{13}{43} \end{array}\right)$$

Theorem. *The convergents* $\frac{p_k}{q_k}$ $\quad \forall k \leq n$ *satisfy:*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$$

Lemma: $q_{k-1} \leq q_k$ for $A \leq k \leq n$ with a strict inequality for $k > 1$. Hence $q_k \longrightarrow \infty$ as $k \longrightarrow \infty$.

Theorem. *The convergents satisfy:*

a) $C_0 < C_2 < C_2 < \ldots$

b) $C_1 < C_3 < C_5 < \ldots$

c) $C_{2s} < C_{2r-1} \quad \forall s \geq 0, r \geq 1.$