# Number Theory, Lecture 13

## Review

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

## Summary

## Summary

## Summary

## Summary

## Summary

## Summary

## Summary

## Congruent modulo $n$

$\mathbb{P} \ni n > 1$.

### Definition

For $a, b \in \mathbb{Z}$, we say that $a$ is congruent to $b$ modulo $n$,

$$a \equiv b \mod n$$

iff $n|(a-b)$.

### Lemma

- $a \equiv a \mod n$,
- $a \equiv b \mod n \iff b \equiv a \mod n$,
- $a \equiv b \mod n \wedge b \equiv c \mod n \implies a \equiv c \mod n$.

**Theorem**

*If* $\gcd(a, n) = 1$ *then*

$$ax \equiv b \mod n$$

*solvable; soln unique modulo* $n$.

## Theorem (CRT)

*If* $\gcd(m,n)=1$, *then the system of eqns*

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned} \tag{CRT}$$

*is solvable; the soln unique modulo* $mn$.

## Example

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 3 \mod 5 \\ x &\equiv 5 \mod 7 \end{aligned}$$

Solve first two eqns:

$$\begin{aligned} x = 1 + 2r &\equiv 3 \mod 2 \\ 2r &\equiv 2 \mod 5 \\ r &\equiv 1 \mod 5 \\ r &= 1 + 5s \\ x = 1 + 2(1 + 5s) &= 3 + 10s \\ x &\equiv 3 \mod 10 \end{aligned}$$

## Example

Now to solve

$$\begin{aligned} x &\equiv 3 \mod 10 \\ x &\equiv 5 \mod 7 \end{aligned}$$

As before:

$$\begin{aligned} x = 3+10s &\equiv 5 \mod 7 \\ 10s &\equiv 2 \mod 7 \\ 5s &\equiv 1 \mod 7 \end{aligned}$$

Find mult inverse of 5 modulo 7:

$$\begin{aligned} s &\equiv 3 \mod 7 \\ s &= 3+7t \\ x = 3+10s &= 3+10(3+7t) \\ &= 33+70t \\ x &\equiv 33 \mod 70 \end{aligned}$$

## Example

Now to solve

$$\begin{aligned} x &\equiv 3 \mod 10 \\ x &\equiv 5 \mod 7 \end{aligned}$$

As before:

$$\begin{aligned} x = 3+10s &\equiv 5 \mod 7 \\ 10s &\equiv 2 \mod 7 \\ 5s &\equiv 1 \mod 7 \end{aligned}$$

Find mult inverse of 5 modulo 7:

$$\begin{aligned} s &\equiv 3 \mod 7 \\ s &= 3+7t \\ x = 3+10s &= 3+10(3+7t) \\ &= 33+70t \\ x &\equiv 33 \mod 70 \end{aligned}$$

## Example

Now to solve

$$\begin{aligned} x &\equiv 3 \mod 10 \\ x &\equiv 5 \mod 7 \end{aligned}$$

As before:

$$\begin{aligned} x = 3+10s &\equiv 5 \mod 7 \\ 10s &\equiv 2 \mod 7 \\ 5s &\equiv 1 \mod 7 \end{aligned}$$

Find mult inverse of 5 modulo 7:

$$\begin{aligned} s &\equiv 3 \mod 7 \\ s &= 3+7t \\ x = 3+10s &= 3+10(3+7t) \\ &= 33+70t \\ x &\equiv 33 \mod 70 \end{aligned}$$

**Theorem (Euler)**

*If* $\gcd(a,n)=1$ *then*

$$a^{\phi(n)} \equiv 1 \mod n \qquad (*)$$

*Equivalently,* $[a]_n^{\phi(n)} = [1]_n \in \mathbb{Z}_n^*$.

Fermat: $n = p$ prime, $p \not| a$, $\phi(p) = p-1$.

## Example

What is the remainder when dividing $1247^{1231}$ with 7?

$$\begin{aligned} 1248^{1231} &\equiv (178*7+2)^{205*6+1} \mod 7 \\ &\equiv 2^{205*6+1} \mod 7 \\ &\equiv 2^{205*6} * 2^1 \mod 7 \\ &\equiv (2^6)^{205} * 2^1 \mod 7 \\ &\equiv 1^{205} * 2^1 \mod 7 \\ &\equiv 2 \mod 7 \end{aligned}$$

**Theorem (Lagrange)**

*$f(x) \in \mathbb{Z}_p[x]$, $\deg(f(x)) = n$. Then $f(x)$ has at most $n$ zeroes in $\mathbb{Z}_p$.*

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, $p$ prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod $p^{r+1}$, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some $t$
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

## Example

$$x^2 + x + 5 \equiv 0 \mod 77$$

Modulo 7: $0 \equiv x^2 - 6x + 5 \equiv (x-3)^2 - 9 + 5 \equiv (x-3)^2 - 4 \equiv (x-3+2)(x-3-2) \equiv (x-1)(x-5)$

Modulo 11: $0 \equiv x^2 - 10x + 5 \equiv (x-5)^2 - 25 + 5 \equiv (x-5)^2 - 9 \equiv (x-5+3)(x-5-3) \equiv (x-2)(x-8)$

Combine using CRT:

$$\left.\begin{array}{l} x \equiv 1 \mod 7 \\ x \equiv 2 \mod 11 \end{array}\right\} \iff x \equiv 57 \mod 77$$

Three more solutions, find them as exercise!

## Lemma (Hensel's lemma)

1. $p$ *prime*
2. $f(x) \in \mathbb{Z}[x]$
3. $f(c) \equiv 0 \mod p^j$
4. $f'(c) \not\equiv 0 \mod p$

*Then there is a unique* $t$ *(mod* $p$*) such that*

$$f(c + tp^j) \equiv 0 \mod p^{j+1}$$

*This* $t$ *is the unique solution to*

$$tf'(c) \equiv \frac{-f(c)}{p^j} \mod p$$

## Example

- $p = 3$
- $f(x) = x^3 + 2$
- $f(1) \equiv 0 \mod 3$
- $f'(x) = 3x^2$, $f'(1) = 3 \equiv 0 \mod 3$
- Hensel: if it lifts, it lifts not uniquely
- In fact no soln modulo 9

## Example

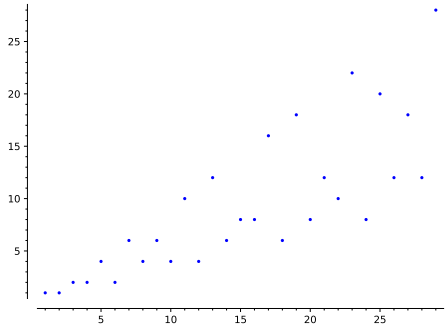
- $p = 5$
- $f(x) = x^3 + 2$
- $f$ has no zeroes in $\mathbb{Z}$ or $\mathbb{Q}$, but one in $\mathbb{R}$, and 3 zeroes in $\mathbb{C}$
- $f(2) \equiv 0 \mod 5$
- $f'(x) = 3x^2$, $f'(2) = 12 \not\equiv 0 \mod 5$
- Hensel: lifts uniquely to all powers of 5
- | $p$ | $p^2$ | $p^3$ | $p^4$ | $p^5$ |
  |---|---|---|---|---|
  | 2 | 22 | 72 | 322 | 947 |

## Definition

An *arithmetical function* is a function $f : \mathbb{P} \to \mathbb{C}$.

We will mostly deal with integer-valued a.f.

Euler $\phi$ is one:



## Arithmetical functions defined by prime factorization

$$n = p_1^{a_1} \cdots p_r^{a_r}, \quad q_i \text{ distinct primes}$$

Liouville function $\lambda$, Möbius function $\mu$:

$$\omega(n) = r$$

$$\Omega(n) = a_1 + \cdots + a_r$$

$$\lambda(n) = (-1)^{\Omega(n)}$$

$$\mu(n) = \begin{cases} \lambda(n) & \omega(n) = \Omega(n) \\ 0 & \text{otherwise} \end{cases}$$

## Arithmetical functions related to divisors

$d$ number of divisors, $\sigma$ sum of divisors, and you know Euler $\phi$.

$$d(n) = \sum_{k|n} 1$$

$$\sigma(n) = \sum_{k|n} k$$

$$\phi(n) = \sum_{\substack{1 \leq k < n \\ \gcd(k,n)=1}} 1$$

## Definition

Let $f, g$ be arithmetical functions. Then their *Dirichlet convolution* is another a.f., defined by

$$(f * g)(n) = \sum_{\substack{1 \leq a,b \leq n \\ ab=n}} f(a)g(b) = \sum_{\substack{1 \leq k \leq n \\ k|n}} f(k)g(n/k) = \sum_{\substack{1 \leq \ell \leq n \\ \ell|n}} f(n/\ell)g(\ell)$$

(DC)

## Example

$$(f * g)(10) = f(1)g(10) + f(2)g(5) + f(5)g(2) + f(10)g(1)$$

## Definition

- $f$ is *totally multiplicative* if $f(nm) = f(n)f(m)$
- $f$ is *multiplicative* if $f(nm) = f(n)f(m)$ whenever $\gcd(n, m) = 1$

## Theorem

*Let $n = \prod_j p_j^{a_j}$, prime factorization. Then*

- *If $f$ mult then either $f = \mathbf{0}$ or $f(1) = 1$ and $f(n) = \prod_j f(p^j)$, i.e., $f$ is determined by its values at prime powers*
- *If $f$ tot mult then $f(n) = \prod_j f(p)^j$, i.e., $f$ is determined by its values at primes*

## Proof.

Obvious! □

## Theorem (Möbius inversion)

1. $\mathbf{1} * \mu = \mathbf{e}$
2. $F(n) = \sum_{k|n} f(k)$ *for all* $n$ *iff* $f(n) = \sum_{k|n} F(k)\mu(n/k)$ *for all* $n$

## Definition

The integer $a$ is a *primitive root* modulo $n$ if $[a]_n$ generates $\mathbb{Z}_n^*$, i.e., if it has multiplicative order $\phi(n)$.

## Example

- 2 is a primitive root modulo 5, since

$$[2]_m^1 = [2],\ [2]_5^2 = [4],\ [2]_5^3 = [3],\ [2]_5^4 = [1]_5$$

- There are not primitive roots modulo 8, since $\mathbb{Z}_8^*$ has $\phi(8) = 4$ elements, but no element has order $> 2$:

| * | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

| * | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

## Theorem

*$p$ prime. Then there exists a primitive root modulo $p$.*

## Proof.

- Ok when $p = 2$
- Assume $p$ odd
- Factor $p - 1 = q_1^{a_1} \cdots q_r^{a_r}$
- $h_1(x) = x^{q_1^{a_1}} - 1$ has exactly $q_1^{a_1}$ roots
- $\hat{h}_1(x) = x^{q_1^{a_1-1}} - 1$ has exactly $q_1^{a_1-1}$ roots
- Exactly $q_1^{a_1} - q_1^{a_1-1}$ elems $v \in \mathbb{Z}_p^*$ with $v^{q_1^{a_1}} = 1$, $v^{q_1^{a_1-1}} \neq 1$
- These fellows have order $q_1^{a_1}$, pick one, $u_1$
- $u = u_1 u_2 \cdots u_r$
- $o(u) = o(u_1) \cdots o(u_r) = q_1^{a_1} \cdots q_r^{a_r} = p - 1$.

□

## Theorem

- *p odd prime*
- $k \in \mathbb{P}$
- *Any primitive root mod* $p^k$ *lifts to* $2p^k$
- *Thus,* $n = 2p^k$ *has primitive roots*
- *Primitive root modulo m iff m is 2, 4,* $p^k$ *or* $2p^2$

## Proof.

Rosen! □

## Definition

- $p$ prime
- $p \not| u$
- $u$ is a quadratic residue modulo $p$ if

$$x^2 \equiv u \mod p$$

is solvable, a quadratic non-residue otherwise

## Example

$p = 5$, squares

| x | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $x^2$ | 0 | 1 | 4 | 4 | 1 |

1,4 q.r, 2,3 q.n.r. 0 square, not q.r.

## Definition

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ q.r. w.r.t. } p \\ -1 & a \text{ q.n.r. w.r.t. } p \\ 0 & a \equiv 0 \mod p \end{cases}$$

Ususually, we only use $a \not\equiv 0 \mod p$. $p$ is still an odd prime.

## Theorem

*$p$ odd prime, $a, b \not\equiv 0 \mod p$. Then*

- $\left(\frac{1}{p}\right) = 1$
- $\left(\frac{a^2}{p}\right) = 1$
- *If* $a \equiv b \mod p$ *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

## Theorem (Euler criterion)

*$p$ odd prime, $P = (p-1)/2$, $a \not\equiv 0 \mod p$. Then*

$$a^P \equiv \left(\frac{a}{p}\right) \mod p$$

## When is $-1$ q.r.?

**Theorem**

$$\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) \equiv (-1)^P \mod p \equiv \begin{cases} +1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

**Theorem**

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$$

## Theorem (Quadratic reciprocity)

*$p, q$ odd primes. Then*

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

## Example

Notation:

$$4+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3+\frac{1}{2}}}}}=[4,2,1,1,3,2]$$

Convergents:

$$[4,]=4, \qquad [4,2]=4+\frac{1}{2}=\frac{9}{2}$$

$$[4,2,1]=4+\cfrac{1}{2+\frac{1}{1}}=\frac{13}{3}, \qquad [4,2,1,1]=4+\cfrac{1}{2+\cfrac{1}{1+\frac{1}{1}}}=\frac{22}{5}$$

$$[4,2,1,1,3]=4+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{3}}}}=\frac{79}{18}$$

$$[4,2,1,1,3,2]=4+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3+\frac{1}{2}}}}}=\frac{180}{41}=\frac{180*4}{41*4}=\frac{720}{164}$$

- Assume $a_0, a_1, \ldots$ are positive real numbers ($a_0$ may be zero)
- For $0 \leq n \leq m$, the $n$th *convergent* of the continued fraction $[a_0, \ldots, a_m]$ is $c_n = [a_0, \ldots, a_n]$. These convergents for $n < m$ are also called *partial convergents*.
- $[a_0, a_1, \ldots, a_{n-1}, a_n] = \left[a_0, a_1, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}\right]$

**Theorem**

*For each $n$ with $-2 \leq n \leq m$, define real numbers $p_n$ and $q_n$ as follows:*

$$\begin{array}{lll} p_{-2} = 0, & p_{-1} = 1, & p_0 = a_0 \\ q_{-2} = 1, & q_{-1} = 0, & q_0 = 1 \end{array}$$

*and for $n \geq 1$,*

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2} \\ q_n &= a_n q_{n-1} + q_{n-2} \end{aligned}$$

*Then, for $n \geq 0$ with $n \leq m$ we have*

$$[a_0, \ldots, a_n] = \frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}$$

*(the last equality for $n \geq 1$)*

## The continued fraction process I

- Let $x \in \mathbb{R}$ and write
$$x = a_0 + t_0$$
with $a_0 \in \mathbb{Z}$ and $0 \leq t_0 < 1$. We call the number $a_0$ the floor of $x$, and we also sometimes write $a_0 = \lfloor x \rfloor$.
- If $t_0 \neq 0$, write
$$\frac{1}{t_0} = a_1 + t_1$$
with $a_1 \in \mathbb{Z}$, $a_1 > 0$, and $0 \leq t_1 < 1$.
- Thus $t_0 = \frac{1}{a_1 + t_1} = [0, a_1 + t_1]$, which is a continued fraction expansion of $t_0$, which need not be simple.

## The continued fraction process II

- Continue in this manner so long as $t_n \neq 0$ writing

$$\frac{1}{t_n} = a_{n+1} + t_{n+1}$$

with $a_{n+1} \in \mathbb{Z}$, $a_{n+1} > 0$, and $0 \leq t_{n+1} < 1$.

- We call this procedure, which associates to a real number $x$ the sequence of integers $a_0, a_1, a_2, \ldots$, the *continued fraction process*.

## Lemma

*For every $n$ such that $a_n$ is defined, we have*

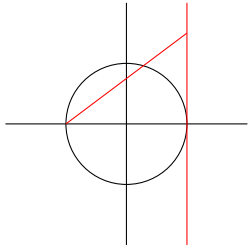
$$x = [a_0, a_1, \ldots, a_n + t_n],$$

*and if $t_n \neq 0$, then $x = [a_0, a_1, \ldots, a_n, \frac{1}{t_n}]$.*

## Theorem

*$(x, y, z)$ is a PPT with $y$ even if and only if there exists integers $0 < n < m$, $m \not\equiv n \mod 2$, such that*

$$x = m^2 - n^2$$
$$y = 2mn$$
$$z = m^2 + n^2$$



**Theorem**

*The positive integer $n = \prod_p p^{a_p}$ can be written as a sum of two squares iff $a_p$ is even for all $p \equiv 3 \mod 4$.*

**Theorem**

*Every positive integer $n$ can be written as the sum of four squares.*

## Definition

- Pell's equation is the Diophantine equation in $x, y$

$$x^2 - dy^2 = 1$$

with $d$ an integer

- Negative Pell is

$$x^2 - dy^2 = -1$$

- We also study the Pell-like equations

$$x^2 - dy^2 = n$$

where $n$ is an integer

## Relation to CF

**Theorem**

*Suppose* $0 < d$, $|n| < \sqrt{d}$, $d$ *not a square. If* $(x, y) \in \mathbb{Z}^2$ *satisfies* $x^2 - dy^2 = n$, *then* $x/y$ *is a convergent of the CF of* $\sqrt{d}$.

**Theorem**

*$d$ positive integer, not square. Then the CF of $\sqrt{d} = [a_0, a_1, a_2, \ldots]$, and the corresponding convergents $p_k/q_k$, can be computed as follows:*

1. $\alpha_0 = \sqrt{d}$, $a_0 = \lfloor \alpha_0 \rfloor$, $P_0 = 0$, $Q_0 = 1$, $p_0 = a_0, q_0 = 1$
2. $\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$, $a_k = \lfloor \alpha_k \rfloor$
3. $P_{k+1} = a_k Q_k - P_k$, $Q_{k+1} = (d - P_{k+1}^2)/Q_k$
4. 

$$P_{k+1} p_k - n q_k = -Q_{k+1} p_{k-1}$$
$$p_k - P_{k+1} q_k = Q_{k+1} q_{k-1}$$

*For all $k$,*

$$p_k^2 - d q_k^2 = (-1)^{k+1} Q_{k+1}$$

## Theorem

*$d$ positive integer, not a square. Let $\sqrt{d} = [a_0, a_1, \dots]$, and let $n$ be the period length of this periodic CF expansion. Let $p_k/q_k$ be the $k$'th convergent.*

- *If $n$ even, negative Pell has no solns, and Pell $x^2 - dy^2 = 1$ has precisely the solns $x = p_{jn-1}$, $y = q_{jn-1}$, $j = 1, 2, 3 \dots$*
- *If $n$ odd, negative Pell has precisely the solns $x = p_{(2j-1)n-1}$, $y = q_{(2j-1)n-1}$, $j = 1, 2, 3, \dots$, and Pell has precisely the solns $x = p_{2jn-1}$, $y = q_{2jn-1}$, $j = 1, 2, 3, \dots$.*

## Definition

$\mathbb{Z}[i] = \{ a + ib | a, b \in \mathbb{Z} \}$

## Lemma

- $\mathbb{Z}[i]$ *subring of* $\mathbb{C}$
- *Not a subfield* ($1/2 \notin \mathbb{Z}[i]$)
- *Integral domain (no zero-divisors)*
- *Principal ideal domain*
- *Euclidean domain*

## Lemma

$\alpha|\beta$ *implies that* $N(\alpha)|N(\beta)$

## Corollary

- $N(\alpha) = 1$ *iff* $\alpha$ *is a unit iff* $\alpha \in \{\pm 1, \pm i\}$
- *if* $N(\alpha)$ *is a (rational) prime, then* $\alpha$ *is irreducible.*

**Theorem (Division algorithm)**

*If* $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, *then exists (not necessarily unique)* $\gamma, \rho \in \mathbb{Z}[i]$ *such that*

1. $\alpha = \gamma\beta + \rho$,
2. $N(\rho) < N(\beta)$, *(in fact, can achieve* $N(\rho) \leq \frac{1}{2}N(\beta)$*)*

## Theorem (Unique factorization)

*If* $0 \neq \alpha \in \mathbb{Z}[i]$, *then*

$$\alpha = \pi_1 \cdots \pi_s$$

*where the* $\pi_i$*'s are Gaussian primes. If furthermore*

$$\alpha = q_1 \cdots q_t$$

*is another factorization of* $\alpha$ *into Gaussian primes, then* $t = s$, *and there is some permutation* $\sigma \in S_s$ *such that* $q_j = \epsilon_j \pi_{\sigma(j)}$ *for* $1 \leq j \leq s$, *with* $N(\epsilon_j) = 1$.

**Theorem**

*Every Gaussian prime $\alpha$ is associate to either*

1. $1+i$
2. $\pi$ *or* $\overline{\pi}$, *where* $N(\pi) = p$ *is a rational prime,* $p \equiv 1 \mod 4$,
3. $p$, *where* $p$ *is a rational prime,* $p \equiv 3 \mod 4$.

## Theorem

*Let the positive integer $n$ have prime factorization*

$$n = 2^m \prod_{j=1}^{s} p_j^{e_j} \prod_{k=1}^{t} q_k^{f_k}$$

*where the $p_j$'s are primes $\equiv 1 \mod 4$, the $q_k$'s are primes $\equiv 3 \mod 4$, and all $f_k$'s are even.*
*Then the number of ways of writing $n$ as a sum of two squares, counting signs and order, is*

$$4 \prod_{j} (e_j + 1)$$

## Example

$$n = 5^2 = (2+i)^2(2-i)^2$$

Possible factors $u + iv$ are

$$(2+i)^2 = 3+4i,\ i(2+i)^2 = -4+3i,\ i^2(2+i)^2 = -3-4i,\ i^3(2+i)^2 = 4-3i,$$
$$(2+i)(2-i) = 5$$
$$(2-i)^2 = 3-4i$$

and 6 more, yielding $n = (\pm 5)^2 + 0^2 = (\pm 3)^2 + (\pm 4)^2 = (\pm 4)^2 + (\pm 3)^2$.

## Example

$$13 = (2+3i)(2-3i),$$

with factors

$$2+3i, -3+2i, -2-3i, 3-2i, 2-3i, 3+2i, -2+3i, -3-2i$$

Hence

$$5^2 * 13 = (2+i)^2(2-i)^2(2+3i)(2-3i),$$

one possible factor is

$$(2+i)^2(2+3i) = (3+4i)(2+3i) = -6+17i$$

so

$$5^2 * 13 = (-6)^2 + 17^2.$$