Lecture 4: gcd, primes, congruence.

Thm For any $a \in \mathbb{Z}$ and non-zero integer b, we have

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

In particular $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = \gcd(a,b)$.

Cor. $\forall a, c \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$,

$$ax + by = c$$

has integer solutions if and only if

$$\gcd(a,b) \mid c.$$

Pf of theorem

In the previous lecture we proved that

(1) $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

(2) If X is a subgroup of $\mathbb{Z}$, then either $X = \{0\}$ or $X = n\mathbb{Z}$ where n is the smallest positive element of X.

Since $b \neq 0$, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ where d is the smallest positive element of $a\mathbb{Z} + b\mathbb{Z}$.

. So $a, b \in d\mathbb{Z} \Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \leq \gcd(a,b)$. (I)

. $\exists\, x, y \in \mathbb{Z}$ s.t. $d = ax + by$ $\Rightarrow \gcd(a,b) \mid d$

$\gcd(a,b) \mid a$, $\gcd(a,b) \mid b$ $\Rightarrow \gcd(a,b) \mid ax+by$

$\Downarrow$

$\gcd(a,b) \leq d$ (II)

(as both of them are positive.)

(I) and (II) $\Rightarrow d = \gcd(a,b)$. ∎

Cor. $c \mid a$ and $c \mid b \Rightarrow c \mid \gcd(a,b)$

Pf. We proved that $\exists\, x, y \in \mathbb{Z}$ s.t.

$\gcd(a,b) = ax + by \Rightarrow c \mid \gcd(a,b)$.

$c \mid a$, $c \mid b$ $\Rightarrow c \mid ax+by$

∎

Cor. $\gcd(a,b) = 1 \iff \exists\, x, y \in \mathbb{Z},\ ax + by = 1$.

(we say a and b are relatively prime.)

Pf. ($\Rightarrow$) Clear by the above theorem.

$\gcd(a,b) \mid ax' + by'$ for any $x', y' \in \mathbb{Z}$

$\Rightarrow \gcd(a,b) \mid 1 \Rightarrow \gcd(a,b) = 1.$

as $\gcd(a,b)$ is positive. ∎

Cor. $\left.\begin{matrix} a \mid bc \\ \gcd(a,b)=1 \end{matrix}\right\} \Rightarrow a \mid c.$

Pf. $\exists x, y \in \mathbb{Z}$, $ax+by=1$

$\Rightarrow acx + bcy = c$

$\left.\begin{matrix} a \mid a \\ a \mid bc \end{matrix}\right\} \Rightarrow a \mid a(cx)+bc(y)=c.$ ∎

Def. An integer $p>1$ is called a prime number if its only divisors are $\pm 1, \pm p$.

Alternatively: $0<d<p$ and $d \mid p \Rightarrow d=1$.

p: prime

Lemma. Let p be a prime number. For any integer n we have either $p \mid n$ or $\gcd(p,n)=1$.

Pf. Let $d=\gcd(p,n)$. So $0<d$ and $d \mid p$. Hence

either $d=1$ or $d=p \Rightarrow d=1$ or $p \mid n$. ■

Cor. $\left.\begin{array}{l} p \text{ : prime} \\ p \mid ab \end{array}\right\} \Rightarrow p \mid a$ or $p \mid b$.

Pf. $p \nmid a \Rightarrow \left.\begin{array}{l} \gcd(p,a)=1 \\ p \mid ab \end{array}\right\} \Rightarrow p \mid b$. ■

Cor. $\left.\begin{array}{l} p \text{ : prime} \\ p \mid a_1 \cdot a_2 \cdots a_n \end{array}\right\} \Rightarrow p \mid a_1$ or $p \mid a_2$ or $\cdots$ or $p \mid a_n$.

Pf proceed by induction on n. ■

The sequence of primes is one of the fascinating integer sequence: they are on one hand highly structured and on the other hand fairly random.

How can we determine all the primes less than X?

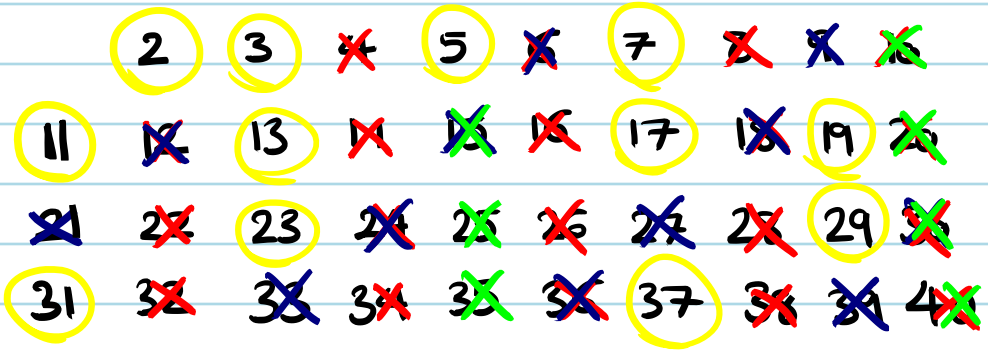
Sieve of Eatosthenes

The key observation is, if n is NOT prime, then it has a divisor $1<a<n \Rightarrow$

$$n=ab$$

for some integers $1<a,b$.

Hence either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. (as otherwise $a > \sqrt{n}$, $b > \sqrt{n} \Rightarrow ab > \sqrt{n} \cdot \sqrt{n} = n$ which is a contradiction.) So to find all the primes ≤ 100, it is enough to cross out all the numbers that have a divisor $\leq \sqrt{100} = 10$.



$n \leq \sqrt{40} \Rightarrow n \leq 6.$

$\{p \mid p \text{ prime and } p \leq 40\} = \{n \in \mathbb{Z} \mid 1 < n \leq 40,$
$2 \nmid n,$
$3 \nmid n,$
$5 \nmid n\} \cup \{2,3,5\}.$

Primes are building blocks of integers in multiplicative sense.

Thm (Fundamental thm of Arithmetic) Any integer $a > 1$ can be uniquely written as $p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ where $p_1 < p_2 < \ldots < p_k$ are prime numbers and $n_1, \ldots, n_k$ are

positive integers.

Pf of FTA. We need to prove the existence and the uniqueness.

Existence. Assume to the contrary that there is an integer >1 which cannot be written as product of prime numbers. I.e.

$$\emptyset \neq \Sigma := \{ n \in \mathbb{Z}^{>1} \mid n \text{ cannot be written as product of prime numbers} \}$$

Hence by the well-ordering principle, Σ has a smallest number n.

Since $n \in \Sigma$, it is NOT a prime number. So $n = ab$ for some integers $1 < a, b < n$.

Since $a, b < n$, $a, b \notin \Sigma$. As $1 < a, b$, a, b can be written as product of prime numbers, which implies that n can be written as product of prime numbers. This contradicts the fact that

$n \in \Sigma$.

Uniqueness Suppose $p_1^{n_1} \cdots p_k^{n_k} = q_1^{m_1} \cdots q_\ell^{m_\ell}$ where $p_1 < \cdots < p_k$ and $q_1 < \cdots < q_\ell$ are prime numbers and $n_1, \ldots, n_k$ and $m_1, \ldots, m_\ell$ are positive integers. Then $k = \ell$, $p_i = q_i$ and $n_i = m_i$.

Pf of Uniqueness

Suppose to the contrary that

$$\emptyset \neq \Sigma = \{ n \in \mathbb{Z}^{>1} \mid n \text{ can be factored as product of primes in two different ways} \}$$

So by the well-ordering principle Σ has a smallest element: $p_1^{n_1} \cdots p_k^{n_k} = q_1^{m_1} \cdots q_\ell^{m_\ell}$

$p_1 \mid \text{LHS} = \text{RHS} \Rightarrow p_1 \mid q_i$ for some i

$\Rightarrow p_1 = q_i$

$q_1 \mid \text{RHS} = \text{LHS} \Rightarrow q_1 \mid p_j$ for some j

$\Rightarrow q_1 = p_j$

$\Rightarrow p_1 = q_1$

$$\Rightarrow p_1^{(n_1-1)} \cdot p_2^{n_2} \cdot \dots \cdot p_k^{n_k} = q_1^{(m_1-1)} \cdot q_2^{m_2} \cdot \dots \cdot q_l^{m_l}$$

and this is NOT in Σ

$\Rightarrow$ So either it is $\underline{1}$ or it can be uniquely written as product of primes. In either case we get contradiction. ■

Thm (Euclid) There are infinitely many prime numbers.

Pf. Suppose to the contrary that there are only finitely many primes: $p_1 < p_2 < \dots < p_n$.

Consider $N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$. Let p be a prime factor of N. So $p = p_i$ for some $i \Rightarrow$

$$\left.\begin{array}{l} p_i \mid p_1 \cdot \dots \cdot p_n + 1 \\ p_i \mid p_i \end{array}\right\} \Rightarrow p_i \mid 1$$ which is a contrad

■