UiO : Universitetet i Oslo

Number Theory

Helmer Aslaksen
Dept. of Teacher Education & Dept. of Mathematics
University of Oslo

helmer.aslaksen@gmail.com
www.math.nus.edu.sg/aslaksen/

Greatest Common Divisor

- We denote the greatest common divisor (or greatest common factor) of m and n by $\gcd(m, n)$ or simply (m, n). If $(m, n) = 1$, we say that m and n are relatively prime or coprime.

Lemma

$\gcd(m - kn, n) = \gcd(m, n)$.

- Proof: If d is a common divisor of m and n, then $m = dm_1$ and $n = dn_1$ so $m - kn = d(m_1 - kn_1)$ and d is also a common divisor of $m - kn$ and n. If d is a common divisor of $m - kn$ and n, then $m - kn = dl$ and $n = dn_1$ so $m = m - kn + kn = d(l + n_1)$ so d is a common divisor of m and n. Since the two pairs have the same common divisors, they also have the same greatest common divisor.
- We can therefore find the gcd by repeatedly subtracting the smaller number from the larger.

Greatest Common Divisor 2

- $$\gcd(7,5) = \gcd(2,5) = \gcd(2,1) = 1.$$
- $1 = 2 - 1 = 2 - (5 - 2 \cdot 2) = 3 \cdot 2 - 1 \cdot 5 = 3(7 - 5) - 1 \cdot 5 = 3 \cdot 7 - 4 \cdot 5.$
- $$\gcd(21,15) = \gcd(6,15) = \gcd(6,3) = 3.$$
- $3 = 6 - 3 = 6 - (15 - 2 \cdot 6) = 3 \cdot 6 - 1 \cdot 15 = 3(21 - 15) - 1 \cdot 15 = 3 \cdot 21 - 4 \cdot 15.$

Bézout's Lemma

- These two examples motivate Bézout's Lemma, named after Étienne Bézout (1730–1783)

Lemma (Bézout's Lemma)

Let d be the smallest positive number that can be written in the form $xm + yn$. Then $d = \gcd(m, n)$.

- We know that the linear combinations of m and n will be multiples of $gcd(m, n)$. The Lemma says that the linear combination are exactly the multiples of $gcd(m, n)$.

Bézout's Lemma 2

- Proof: If we divide m by d, we subtract multiples of d from m, so the remainder will be of the form $am + bn$. But since the remainder is less that d, and d is the smallest positive number of this form, the remainder must be zero, so d divides m. The same argument applies to n, so d is a common divisor of m and n.
- Let c any common divisor of m and n. Then $m = cm_1$ and $n = cn_1$, so $d = xm + yn = c(xm_1 + yn_1)$, so c must also be a divisor of d. Hence d is the greatest common divisor.

The Fundamental Theorem of Arithmetic

- $p > 1$ is prime number if its only factors are 1 and p.

Theorem (The Fundamental Theorem of Arithmetic)

For $n > 1$ there is a unique expression

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < p_2 < \cdots < p_r$ are prime numbers and each $k_i \geq 1$.

- The reason why we do not want 1 to be a prime number, is to ensure uniqueness in this decomposition.

Proof of FTA

- Proof of existence: If n is prime, the theorem is true. If not, we can write $n = ab$, and consider a and b separately. In this way we get a product of smaller and smaller factors, but this process must stop, which it does when the factors are primes. This was proved by Euclid around 300 BCE.
- In order to prove uniqueness, we first need a property of prime numbers.

Proof of FTA 2

- We write $m|n$ if m divides n.

Lemma

Let p be a prime number. If $p|mn$, then $p|m$ or $p|n$.

- Proof: Assume that $p \not| m$. Then $\exists x, y$ such that $xp + ym = 1$.
- Then $xpn + ymn = n$, and it follows that $p|n$.
- This fails if p is not prime, since $6|3 \cdot 4$ without 6 dividing any of the factors.

Proof of FTA 3

- Proof of uniqueness: Suppose the decomposition is not unique. After cancelling common factors, we can then assume that

  $$p_1 \cdots p_k = q_1 \cdots q_l,$$

  where $p_i \neq q_j$ for all i and j.
- It then follows from our lemma that p_1 either divides q_1, which is impossible since we assumed that p_1 is not equal to q_1, or p_1 divides $q_2 \cdots q_l$. Applying the lemma again, we eventually get a contradiction.

Least Common Multiple

- We denote the least common multiple of m and n by $\mathrm{lcm}(m, n)$.
- If $m = p_1^{a_1} \cdots p_k^{a_k}$ and $n = p_1^{b_1} \cdots p_k^{b_k}$, then

$$\gcd(m, n) = p_1^{\min(a_1, b_1)} \cdots p_k^{\min(a_k, b_k)}$$

and

$$\mathrm{lcm}(m, n) = p_1^{\max(a_1, b_1)} \cdots p_k^{\max(a_k, b_k)},$$

and since $\max(a, b) + \min(a, b) = a + b$, we have

$$\gcd(m, n) \cdot \mathrm{lcm}(m, n) = mn.$$

Modular Arithmetic

- We will say that $a \equiv b \pmod{n}$ or $\bar{a} = \bar{b}$ if n divides $a - b$, which we will denote by $n | (a - b)$.
- Let $\mathbb{Z}_n = \{\bar{0}, \ldots, \overline{n-1}\}$ be the set of congruence classes mod n.

Fermat's Little Theorem

- **Theorem (Fermat's Little Theorem)**

  If $p \not| a$, then $a^{p-1} \equiv 1 \pmod p$.

  - Proof: Consider the set of nonzero congruence classes $\{\bar{1}, \dots, \overline{p-1}\}$ and the set $\{\bar{a}\bar{1}, \dots, \bar{a}(\overline{p-1})\}$.
  -

$$a \cdot i \equiv a \cdot j \pmod p$$
$$a(i-j) \equiv 0 \pmod p.$$

Since $p \not| a$, this can only happen if $i = j$, so the two sets of classes are the same.

Fermat's Little Theorem 2

- We multiply the elements of the two sets together and get

$$\begin{aligned}
(a \cdot 1) \cdots (a \cdot (p-1)) &\equiv 1 \cdots (p-1) \pmod{p} \\
a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\
a^{p-1} &\equiv 1 \pmod{p},
\end{aligned}$$

since $(p-1)! \not\equiv 0 \pmod{p}$.

Euler's ϕ function

- In 1763, Leonhard Euler (1707–1783) introduced the function

$$\phi(n) = \text{Number of } 1 \leq k \leq n \text{ with } \gcd(k, n) = 1.$$

- We have $\phi(p) = p - 1$.
- In general

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right),$$

since the only numbers less than or equal to p^k that are relatively prime to p^k are xp for $1 \leq x \leq p^{k-1}$.

Euler's ϕ function 2

- We will prove that ϕ is multiplicative, meaning that

$$(m, n) = 1 \implies \phi(mn) = \phi(m)\phi(n).$$

- Consider $m = 5$ and $n = 7$. Then the numbers less than or equal to 35 that are not coprime with 35 are the 11 multiples of 5 and 7 less than or equal to 35, i.e. 5, 7, 10, 14, 15, 20, 21, 25, 28, 30, 35.
- It follows that $\phi(35) = 35 - 11 = 24 = 4 \cdot 6 = \phi(5)\phi(7)$

Euler's ϕ function 3

- We will first need a lemma.

Lemma

Assume that $(a, b) = 1$*. Then*

$$(a, y) = 1 \wedge (b, x) = 1 \iff (ax + by|ab) = 1.$$

- Proof: Suppose there is a $p > 1$ such that $p|(ax + by, ab)$. Then $p|ab$ and we know that $p|a$ or $p|b$. Assume that $p|a$. Then $p|y$, so $(a, y) > 1$. Similarly if $p|b$.
- Suppose that $(b, x) > 1$. Since $(b, x)|ax + by$, we have $(ax + by, ab) > 1$. Similarly $(a, y) > 1$ also implies $(ax + by, ab) > 1$.

Euler's Theorem

- **Theorem (Euler's Theorem)**

  If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

  - The proof is similar to the proof of Fermat's Little Theorem, of which it is a generalization, since $\phi(p) = p - 1$. Instead of considering the set of nonzero congruence classes, we consider the set $\{\overline{c_1}, \ldots, \overline{c_{\phi(n)}}\}$ of congruence classes corresponding to c with $(c, n) = 1$.
  - We will call $\overline{a} \in \mathbb{Z}_n$ a unit if it has an inverse, i.e., there is $\overline{b} \in \mathbb{Z}_n$ such that $ab \equiv 1 \pmod{n}$.

Lemma

$\overline{a}$ is a unit in $\mathbb{Z}_n$ if and only if $(a, n) = 1$.

- If $(a, n) = 1$, we use Euler's Theorem and set $b = a^{\phi(n)-1}$. If a is a unit, we can find b and k such that $ab - 1 = kn$ or $ab - kn = 1$, so $(a, n) = 1$.

Order of an element

- If $a \in \mathbb{Z}_n$ is a unit, we will say that the *order* of a is the smallest positive number k such that $a^k \equiv 1 \pmod{n}$.

Lemma

If $(a, n) = 1$ and k is the order a, then $k | \phi(n)$.

- Proof: We know that $a^{\phi(n)} \equiv 1 \pmod{n}$. Suppose that $\phi(n) = lk + r$, where $0 \leq r < k$. Then

$$1 \equiv a^{\phi(n)} \equiv a^{lk+r} \equiv (a^k)^l a^r \equiv a^r \pmod{n},$$

but since k is smallest positive number with $a^k \equiv 1 \pmod{n}$, we must have $r = 0$, so $k | \phi(n)$.