



UiO : University of 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/](http://www.math.nus.edu.sg/aslaksen/)



UiO : University of Oslo

## Greatest Common Divisor

- ▶ We denote the greatest common divisor (or greatest common factor) of  $m, n \in \mathbb{N}$  by  $\gcd(m, n)$  or simply  $(m, n)$ . If  $(m, n) = 1$ , we say that  $m$  and  $n$  are relatively prime or coprime.
- ▶ If we know the prime factorization of  $m = p_1^{a_1} \cdots p_r^{a_r}$  and  $n = p_1^{b_1} \cdots p_r^{b_r}$ , then  $(m, n) = p_1^{c_1} \cdots p_r^{c_r}$  where  $c_i = \min(a_i, b_i)$ . Notice that some of the  $a_i, b_i$  and  $c_i$  may be 0.
- ▶ Unfortunately, factorization is computationally hard, so we need a way to compute gcd without factoring.
- ▶ This is given by the Euclidean Algorithm (ca 300 BCE).

## Greatest Common Divisor 2

- ▶ The basic idea is the following Lemma:

### Lemma

$\gcd(m - kn, n) = \gcd(m, n)$  for  $k, m, n \in \mathbb{N}$ .

- ▶ For example, we have

$$\begin{aligned} (54, 24) &= (54 - 2 \cdot 24, 24) = (6, 24) \\ &= (6, 24 - 4 \cdot 6) = (6, 0) = 6. \end{aligned}$$

- ▶ Note that since  $n \cdot 0 = 0$ , any number is a divisor of 0, so  $(n, 0) = n$ .
- ▶ Since division is just repeated subtraction, we can at each step replace  $(a, b)$ , with  $a \geq b$ , by  $(\text{mod}(a, b), b)$ , where  $\text{mod}(a, b)$  denotes the remainder when dividing  $a$  by  $b$ .
- ▶ The Euclidean Algorithm consists simply in repeated application of this idea until one number becomes 0, at which stage the other number is the gcd.

## Greatest Common Divisor 3

- ▶ Let us consider a nontrivial example where  $m = 41 \cdot 51 = 2091$  and  $n = 43 \cdot 47 = 2021$ .
- ▶

$$\begin{aligned} &(2091, 2021) \\ &= (2091 - 2021, 2021) = (70, 2021) \\ &= (70, 2021 - 28 \cdot 70) = (70, 2021 - 1960) = (70, 61) \\ &= (70 - 61, 61) = (9, 61) \\ &= (9, 61 - 6 \cdot 9) = (9, 7) \\ &= (9 - 7, 7) = (2, 7) \\ &= (2, 7 - 3 \cdot 2) = (2, 1) \\ &= (2 - 2 \cdot 1, 1) = (0, 1) = 1. \end{aligned}$$

- ▶ Notice the way the two numbers decrease. The smallest number becomes the largest number, and then gets “divided away” to be replaced by a new smallest number.

## Greatest Common Divisor 4

- ▶ Let us now prove our Lemma.
- ▶ 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. □

## Greatest Common Divisor 5

- ▶ We can also run the steps in the algorithm backwards. This enables us to express the gcd as a linear combination of the two numbers.

$$(7, 5) = (2, 5) = (2, 1) = (0, 1) = 1.$$

- ▶  $1 = 2 - 1 = 2 - (5 - 2 \cdot 2) = 3 \cdot 2 - 1 \cdot 5 = 3(7 - 5) - 1 \cdot 5 = 3 \cdot 7 - 4 \cdot 5.$



$$(21, 15) = (6, 15) = (6, 3) = (0, 3) = 3.$$

- ▶  $3 = 6 - 3 = 6 - (15 - 2 \cdot 6) = 3 \cdot 6 - 1 \cdot 15 = 3(21 - 15) - 1 \cdot 15 = 3 \cdot 21 - 4 \cdot 15.$
- ▶ The Euclidean Algorithm will both give us the gcd and express the gcd as a linear combination of the two numbers.

## Greatest Common Divisor 6

- ▶ We will define,  $I(m, n)$ , the ideal generated by  $m$  and  $n$  to be the set of integral linear combinations of  $m$  and  $n$ ,  $\{xm + yn \mid x, y \in \mathbb{Z}\}$ .
- ▶ If  $d = (m, n)$ , and we denote the set of integral multiples of  $d$  by  $I(d)$ , then we have  $I(m, n) \subseteq I(d)$ , since a linear combination of  $m$  and  $n$  is also a multiple of  $d$ .
- ▶ However, if we run the Euclidean Algorithm backwards, we see that we can express  $d$  as a linear combination of  $m$  and  $n$ , and that shows that  $I(d) \subseteq I(m, n)$ , so these two sets are in fact equal, and we have proved the following theorem.

### ▶ Theorem

*For  $m, n \in \mathbb{Z}$  we have*

$$\{xm + yn \mid x, y \in \mathbb{Z}\} = \{z \operatorname{gcd}(m, n) \mid z \in \mathbb{Z}\}.$$

## Bézout's Lemma

- ▶ This fact can be restated in a useful form known as Bézout's Lemma, named after Étienne Bézout (1730–1783).

### Lemma (Bézout's Lemma)

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

- ▶ This lemma gives an alternative characterization of the gcd. It is a consequence of the previous Theorem, since  $c$  is the smallest positive number on the left, and  $d$  is the smallest positive number on the right.

## Proof of Bézout's Lemma

- ▶ We will also give a direct proof.
- ▶ Proof: If we divide  $m$  by  $c$ , we subtract multiples of  $c$  from  $m$ , but since  $c$  is a linear combination of  $m$  and  $n$ , the remainder will also be a linear combination of  $m$  and  $n$ .
- ▶ But since the remainder is less than  $c$ , and  $c$  is the smallest positive number of this form, the remainder must be zero, so  $c$  divides  $m$ .
- ▶ The same argument applies to  $n$ , so  $c$  is a common divisor of  $m$  and  $n$ .
- ▶ Let  $k$  any common divisor of  $m$  and  $n$ . Then  $m = km_1$  and  $n = kn_1$ , so  $c = xm + yn = k(xm_1 + yn_1)$ , so  $k$  must also be a divisor of  $c$ . Hence  $c$  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*

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

*where  $p_1 < p_2 < \dots < p_r$  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, and  $m, n \in \mathbb{N}$ . If  $p|mn$ , then  $p|m$  or  $p|n$ .*

- ▶ Proof: Assume that  $p \nmid m$ . Then  $(p, m) = 1$ , so  $\exists x, y$  such that  $xp + ym = 1$ .
- ▶ Then  $xpn + ymn = n$ , and since  $p|mn$ , 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  $\text{lcm}(m, n)$ .
- ▶ If  $m = p_1^{a_1} \cdots p_k^{a_k}$  and  $n = p_1^{b_1} \cdots p_k^{b_k}$ , then

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

and

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

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

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

$$\text{lcm}(m, n) = \frac{mn}{\text{gcd}(m, n)}.$$

- ▶ This shows that  $\text{lcm}(m, n) = mn$  precisely when  $\text{gcd}(m, n) = 1$ .

## Modular Arithmetic

- ▶ We will say that  $a \equiv b \pmod{n}$  or  $\bar{a} = \bar{b}$  if  $n$  divides  $a - b$ .
- ▶ Let  $\mathbb{Z}_n = \{\bar{0}, \dots, \overline{n-1}\}$  be the set of congruence classes mod  $n$ .
- ▶ Let us compute the multiplication table for  $\mathbb{Z}_3$ .

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

## Modular Arithmetic 2

- ▶ Let us compute the multiplication table for  $\mathbb{Z}_5$ .

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- ▶ Notice that

$$\bar{2}^2 = \bar{4}, \quad \bar{2}^3 = \bar{3}, \quad \bar{2}^4 = \bar{1},$$

$$\bar{3}^2 = \bar{4}, \quad \bar{3}^3 = \bar{2}, \quad \bar{3}^4 = \bar{1},$$

$$\bar{4}^2 = \bar{1}, \quad \bar{4}^3 = \bar{4}, \quad \bar{4}^4 = \bar{1}.$$



## Modular Arithmetic 3

- ▶ We will call  $\bar{a} \in \mathbb{Z}_n$  a unit if it has an inverse, i.e., there is  $\bar{b} \in \mathbb{Z}_n$  such that  $\bar{a}\bar{b} = \bar{1}$ .

### Lemma

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



$$\begin{aligned} (a, n) = 1 &\iff \exists b, c \text{ such that } ba + cn = 1 \\ &\iff ba - 1 = -cn \iff \bar{a}\bar{b} = \bar{1}. \quad \square \end{aligned}$$

- ▶ It follows that if  $p$  is prime, then for any  $\bar{a} \in \mathbb{Z}_p$  with  $1 \leq a \leq p - 1$  we have  $(a, p) = 1$ , and it follows that all  $\bar{a} \neq \bar{0}$  are units in  $\mathbb{Z}_p$ .
- ▶ If  $p$  is prime, then  $\mathbb{Z}_p$  is a field. That means that we can add and multiply, and all non-zero elements have a multiplicative inverse.
- ▶ If  $a$  is invertible, then the equation  $\bar{a}\bar{x} = \bar{b}$  has the solution  $\bar{x} = \bar{a}^{-1}\bar{b}$ .

## Modular Arithmetic 3

- ▶ Let us compute the multiplication table for  $\mathbb{Z}_6$ .

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- ▶ Notice that  $\bar{5}$  is the only unit, and that its row is a permutation of the classes.
- ▶ Notice that  $\{\bar{0}, \bar{3}\}$  and  $\{\bar{0}, \bar{2}, \bar{4}\}$  are closed under addition and multiplication.
- ▶ Since  $(n - 1, n) = 1$  and  $(n - 1)i \equiv -i \equiv n - i \pmod{n}$ , we see that the last row in the multiplication table of  $\mathbb{Z}_n$  will always be the classes in decreasing order.

## Fermat's Little Theorem

### ▶ Theorem (Fermat's Little Theorem)

Let  $p$  be a prime number. If  $p \nmid a$ , 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  $\{\bar{a}\bar{1}, \dots, \bar{a}\overline{(p-1)}\}$ .



$$\begin{aligned} a \cdot i &\equiv a \cdot j \pmod{p} \\ a(i - j) &\equiv 0 \pmod{p}. \end{aligned}$$

Since  $p \nmid a$ , this can only happen if  $\bar{i} = \bar{j}$ , 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  $(p-1)! \not\equiv 0 \pmod{p}$ .



## Fermat's Little Theorem 3

- ▶ We can also write this as  $a^p \equiv a \pmod{p}$ . In this form, the statement is also true for  $a = kp$ . For small values we can see this directly.
- ▶  $a^2 - a = a(a - 1)$  is always divisible by 2, since in the product of two consecutive integers, one of the factors must be even.
- ▶ Similarly,  $a^3 - a = a(a^2 - 1) = (a + 1)a(a - 1)$  is always divisible by 3, since in the product of three consecutive integers, one of the factors must be divisible by 3.

## Euler's $\phi$ function

- ▶ In 1763, Leonhard Euler (1707–1783) defined  $\phi(n)$  to be the number of integers  $k$  with  $1 \leq k \leq n$  and  $\gcd(k, n) = 1$ .
- ▶ We have  $\phi(p) = p - 1$  for any prime number  $p$ .
- ▶ 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 not relatively prime to  $p^k$  are  $xp$  for  $1 \leq x \leq p^{k-1}$ .

Euler's  $\phi$  function 2

- ▶ We will prove that  $\phi$  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  $\phi$  function 3

- ▶ We will first need a lemma.

## Lemma

Assume that  $(m, n) = 1$ . Then

$$\gcd(m, y) = 1 \wedge \gcd(n, x) = 1 \iff \gcd(mx + ny, mn) = 1.$$

- ▶ Proof (optional): Suppose there is a  $p > 1$  such that  $p|(mx + ny, mn)$ . Then  $p|mn$  and we know that  $p|m$  or  $p|n$ . Assume that  $p|m$ . Then  $p|y$ , so  $(m, y) > 1$ . Similarly if  $p|n$ .
- ▶ Suppose that  $(n, x) > 1$ . Since  $(n, x)|mx + ny$ , we have  $(mx + ny, mn) > 1$ . Similarly  $(m, y) > 1$  also implies  $(mx + ny, mn) > 1$ . □

Euler's  $\phi$  function 4

- ▶ We can now easily prove the theorem.

## Theorem

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

- ▶ Proof (optional): Suppose that  $x$  ranges through the  $\phi(n)$  numbers coprime to  $n$  and  $y$  ranges through the  $\phi(m)$  numbers coprime to  $m$ . Then  $mx + ny$  ranges through the  $\phi(m)\phi(n)$  numbers coprime to  $mn$ , which equals  $\phi(mn)$ . □
- ▶ It now follows that if  $n = p_1^{a_1} \cdots p_k^{a_k}$ , then

$$\begin{aligned} \phi(n) &= \phi(p_1^{a_1} \cdots p_k^{a_k}) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) \\ &= p_1^{a_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{a_k} \left(1 - \frac{1}{p_k}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \end{aligned}$$

## Euler's Theorem

- ▶ We can generalize Fermat's Little Theorem as follows.

## Theorem (Euler's Theorem)

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

- ▶ Proof: 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  $\{\overline{c_1}, \dots, \overline{c_{\phi(n)}}\}$  of congruence classes corresponding to  $c$  with  $(c, n) = 1$ . □

## Euler's Theorem 2

- ▶ For  $n = 5$ , we get that  $\phi(5) = 4$  and  $\bar{2}^4 = \bar{3}^4 = \bar{4}^4 = \bar{1}$ , but notice that  $\bar{4}^2 = \bar{1}$ , too.
- ▶ For  $n = 6$ , we get that  $\phi(6) = 2$  and  $\bar{5}^2 = \bar{1}$ .
- ▶ For  $n = 8$ , we get that  $\phi(8) = 4$  and  $\bar{3}^4 = \bar{5}^4 = \bar{7}^4 = \bar{1}$ , but notice that  $\bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1}$ , too.

## Order of an element

- ▶ If  $\bar{a} \in \mathbb{Z}_n$  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  $\gcd(a, n) = 1$  and  $k$  is the order  $a$ , then  $k \mid \phi(n)$ .

- ▶ 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  $k \mid \phi(n)$ . □

- ▶ In  $\mathbb{Z}_5$ , the orders of  $\bar{2}$  and  $\bar{3}$  are  $\phi(5) = 4$ , but the order of  $\bar{4}$  is 2.
- ▶ In  $\mathbb{Z}_6$ , the order of  $\bar{5}$  is  $\phi(6) = 2$ .
- ▶ In  $\mathbb{Z}_8$ , the orders of  $\bar{3}$ ,  $\bar{5}$  and  $\bar{7}$  are  $2 = \phi(8)/2$ .