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/

Greatest Common Divisor 1

- 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 $\gcd(m, n) = 1$, we say that m and n are coprime or relatively prime.
- 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 $\gcd(m, n) = p_1^{c_1} \cdots p_r^{c_r}$ 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

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

- Note that since $n \cdot 0 = 0$, any number is a divisor of 0, so $\gcd(n, 0) = n$.
- Since division is just repeated subtraction, we can at each step replace $\gcd(a, b)$, with $a > b$, by $\gcd(\text{mod}(a, b), b)$, where $\text{mod}(a, b)$ denotes the remainder when dividing a by b.
- The Euclidean Algorithm consists simply of 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 $n = 43 \cdot 47 = 2021$.
- $$\begin{aligned} &\gcd(2091, 2021) \\ &= (2091 - 2021, 2021) = (70, 2021) \\ &= (70, 2021 - 28 \cdot 70) = (70, 2021 - 1960) = (70, 61) \\ &= (70 - 61, 61) = (9, 61) \\ &= (9, 61 - 6 \cdot 9) = (9, 7) \\ &= (9 - 7, 7) = (2, 7) \\ &= (2, 7 - 3 \cdot 2) = (2, 1) \\ &= (2 - 2 \cdot 1, 1) = (0, 1) = 1. \end{aligned}$$
- 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 $m = m - kn + kn = d(l + kn_1)$ 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. $\square$

Greatest Common Divisor 5

- We can also run the steps in the algorithm backwards. At each step we divide a by b and get a remainder r, satisfying $a = k \cdot b + r$. This can be written as $r = a - k \cdot b$, so at each step the new number can be written as a combination of the two previous numbers. This enables us to recursively express the gcd as a linear combination of the two numbers.

Greatest Common Divisor 6

- We have

$$\gcd(7,5) = (2,5) = (2,1) = (0,1) = 1$$

  since

$$7 = 1 \cdot 5 + 2, \quad 5 = 2 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0.$$

  We start with the last equation before we get 0, namely $5 = 2 \cdot 2 + 1$. We can write it as $1 = 5 - 2 \cdot 2$, which expresses the gcd, 1, as a combination of the two previous numbers, 2 and 5. But the previous equation, $7 = 1 \cdot 5 + 2$, shows that 2 can be expressed in terms of 7 and 5.
- Hence

$$\gcd(7,5) = 1 = 5 - 2 \cdot 2 = 5 - 2(7-5) = 3 \cdot 5 - 2 \cdot 7.$$

Greatest Common Divisor 7

- We have

$$\gcd(21, 15) = (6, 15) = (6, 3) = (0, 3) = 3,$$

  and hence

$$\gcd(21, 15) = 3 = 15 - 2 \cdot 6 = 15 - 2(21 - 15) = 3 \cdot 15 - 2 \cdot 21.$$

- The Euclidean Algorithm will both give us the gcd and express the gcd as a linear combination of the two numbers.

Greatest Common Divisor 8

- 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

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

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 $c = \gcd(m, n)$.

- 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.
- Notice that if $\gcd(m, n) = 1$, then any integer can be written as a linear combination of m and n.

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 that 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. $\square$

Prime Numbers 1

- Let S be a set of numbers. We will say that $a \in S$ is invertible in S if it has a multiplicative inverse in S, i.e., there exists a $b \in S$ such that $ab = 1$. Notice that 2 is invertible in $\mathbb{Q}$, since $1/2 \in \mathbb{Q}$, but 2 is not invertible in $\mathbb{Z}$, since $1/2 \notin \mathbb{Z}$.
- The invertible elements in $\mathbb{Z}$ are 1 and -1, while 1 is the only invertible element in $\mathbb{N}$.
- $p \in \mathbb{N}$ is prime if it is not invertible, and cannot be written as a product of two non-invertible elements. This is the same as saying that $p > 1$ and the only divisors are 1 and p.
- Notice that 1 is not a prime number, since it is invertible. The point of this "complicated" definition of a prime is to motivate why 1 is not a prime.
- Notice that 2 is the only even prime.

Prime Numbers 2

- Euclid proved that there are infinitely many prime numbers.
- Let $p_1, \ldots, p_n$ be prime numbers and set $N = p_1 \cdot \cdots \cdot p_n + 1$. Then N is not divisible by any of the p_i. Therefore either N is itself prime, or N is divisible by some other prime number.
- In either case, there must be another prime number in addition to the p_i, so there cannot be a finite list of primes.
- Notice that N does not have to be prime. For example $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 509 \cdot 59$.

The Fundamental Theorem of Arithmetic 1

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 $k_i \geq 1$.

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

The Fundamental Theorem of Arithmetic 2

- 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. $\square$
- In order to prove uniqueness, we first need a property of prime numbers.

The Fundamental Theorem of Arithmetic 3

- 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 $p \not| m$. Then $\gcd(p, m) = 1$, and we can find x and y such that $xp + ym = 1$.
- Then $xpn + ymn = n$, and since $p|mn$, it follows that $p|n$. $\square$
- This fails if p is not prime, since $6|(3 \cdot 4)$ without 6 dividing either 3 or 4.

The Fundamental Theorem of Arithmetic 4

- Proof of uniqueness: Suppose the decomposition is not unique. After canceling 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. $\square$

Least Common Multiple

- We denote the least common multiple of m and n by $\operatorname{lcm}(m,n)$.
- 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

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

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

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

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

Modular Arithmetic 1

- We will say that $a \equiv b \pmod{n}$ if n divides $a - b$, which means that a and b have the same remainder when we divide by n.
- We write $\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$ to denote the set of integers that are equivalent to a and call this the congruence class of a.
- Since every number is congruent mod n to a number between 0 and $n - 1$, we can write $\mathbb{Z}_n = \{\overline{0}, \dots, \overline{n-1}\}$ to denote the set of congruence classes mod n.

Modular Arithmetic 2

- We now define addition and multiplication of congruence classes by setting

$$\overline{a} + \overline{b} = \overline{a + b},$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

- The important part about this definition is that it is “well-defined” in the sense that it does not matter which representative we choose of each class.
- For instance, if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ so $\overline{a_1 + b_1} = \overline{a_2 + b_2}$.

Modular Arithmetic 3

- Let us compute the multiplication table for $\mathbb{Z}_2$.

	0	1
0	0	0
1	0	1

- Can you express in words what this table says about multiplication of odd and even numbers?
- 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 4

- 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

$$\begin{aligned}
\overline{2}^2 &= \overline{4}, & \overline{2}^3 &= \overline{3}, & \overline{2}^4 &= \overline{1}, \\
\overline{3}^2 &= \overline{4}, & \overline{3}^3 &= \overline{2}, & \overline{3}^4 &= \overline{1}, \\
\overline{4}^2 &= \overline{1}, & \overline{4}^3 &= \overline{4}, & \overline{4}^4 &= \overline{1}.
\end{aligned}$$

Modular Arithmetic 5

- We will say that $\overline{a} \in \mathbb{Z}_n$ is invertible if it has a multiplicative inverse, i.e., there is $\overline{b} \in \mathbb{Z}_n$ such that $\overline{a}\,\overline{b} = \overline{1}$.

Lemma

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

-

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

- It follows that if p is prime, then for any $\overline{a} \in \mathbb{Z}_p$ with $1 \leq a \leq p - 1$ we have $\gcd(a, p) = 1$, and it follows that all $\overline{a} \neq \overline{0}$ are invertible in $\mathbb{Z}_p$.

Modular Arithmetic 6

- Notice that if p is prime, then in $\mathbb{Z}_p$ we can add, multiply and subtract, and that all non-zero elements have a multiplicative inverse. This is not true for $\mathbb{Z}$, since $1/2 \notin \mathbb{Z}$, and is one of the main reasons why we are interested in $\mathbb{Z}_p$.
- If a is invertible, then the equation $\overline{a}\,\overline{x} = \overline{b}$ has the solution $\overline{x} = \overline{a}^{-1}\overline{b}$.

Modular Arithmetic 7

- 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 $\overline{5}$ is the only invertible element, and that its row is a permutation of the classes.
- Notice that $\{\overline{0}, \overline{3}\}$ and $\{\overline{0}, \overline{2}, \overline{4}\}$ are closed under addition and multiplication.
- Since $\gcd(n-1, n) = 1$ 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.

Divisibility tests

- We will now show how we can use modular arithmetic to derive divisibility tests.

Divisibility by 3 or 9

Theorem

A number is divisible by 3 (or 9) if and only if its digit sum is divisible by 3 (or 9).

$$3 | \sum_{i=0}^{n} a_i 10^i \Leftrightarrow 3 | \sum_{i=0}^{n} a_i,$$
$$9 | \sum_{i=0}^{n} a_i 10^i \Leftrightarrow 9 | \sum_{i=0}^{n} a_i.$$

- Proof: Since $10 \equiv 1 \pmod 3$ and $\pmod 9$, we have

$$\sum a_i 10^i \equiv \sum a_i 1^i \equiv \sum a_i \pmod 3 \quad \text{and} \quad \pmod 9. \qquad \square$$

Divisibility by 3 or 9

- $$111{,}111{,}093 \equiv 18 \equiv 9 \equiv 0 \pmod 9,$$

  so 9 divides 111,111,093.

Divisibility by 4

Theorem

A number, $100c + d$, where d is the last two digits, is divisible by 4 if and only if the last two digits are divisible by 4.

- Proof: We have

$$100c + d \equiv d \pmod 4. \qquad \square$$

Divisibility by 4

- $$111{,}111{,}092 \equiv 92 \pmod{4},$$

  so 4 divides 111,111,092.

Divisibility by 7 1

Theorem

A number, $10a + b = 100c + d = \sum_{i=0}^{n} a_i(1{,}000)^i$*, where b is the last digit, d is the last two digits, and the* a_i*'s are blocks of digits of length three starting from the right, is divisible by 7 if and only if 7 divides* $a + 5b$*,* $2c + d$ *or* $\sum_{i=0}^{n}(-1)^i a_i$*.*

$$7|10a + b \Leftrightarrow 7|a + 5b,$$
$$7|100c + d \Leftrightarrow 7|2c + d,$$
$$7|\sum_{i=0}^{n} a_i(1{,}000)^i \Leftrightarrow 7|\sum_{i=0}^{n}(-1)^i a_i.$$

Divisibility by 7 2

- Proof: We have

$$5(10a + b) \equiv 49a + a + 5b \equiv a + 5b \pmod 7,$$

which is 0 if and only if $10a + b \equiv 0 \pmod 7$, since 5 is invertible in $\mathbb{Z}_7$.

- The second part follows from

$$100c + d \equiv (98 + 2)c + d \equiv 2c + d \pmod 7.$$

- The last part follows from $10^3 \equiv 3^3 \equiv 27 \equiv -1 \pmod 7$, which gives

$$\sum_{i=0}^{n} a_i (1{,}000)^i \equiv \sum_{i=0}^{n} (-1)^i a_i \pmod 7. \qquad \square$$

Divisibility by 7 3

- $$86{,}419{,}746 = 10 \cdot 86{,}419{,}74 + 6 = 100 \cdot 864{,}197 + 46 = 86 \cdot 10^6 + 419 \cdot 10^3 + 746 \cdot 10^0.$$

- $$\begin{aligned} 86{,}419{,}74 + 5 \cdot 6 &= 8{,}642{,}004, \\ 8{,}642{,}00 + 5 \cdot 4 &= 864{,}220, \\ 86{,}422 + 5 \cdot 0 &= 86{,}422, \\ 8{,}642 + 5 \cdot 2 &= 8{,}652, \\ 865 + 5 \cdot 2 &= 875, \\ 87 + 5 \cdot 5 &= 112, \\ 11 + 5 \cdot 2 &= 21, \\ 2 + 5 \cdot 1 &= 7. \end{aligned}$$

  so 7 divides 86,419,746.

Divisibility by 7 4

- $$86{,}419{,}746 \equiv 86 - 419 + 746 \equiv 413 \pmod 7,$$

  and 7 divides 413 so so 7 divides 86,419,746.
- The first method is simple, but requires a lot of computations. The second method requires only half as much computation, but the $2c$ term requires more computation.
- The most efficient is probably a combination. In our example, we could for example use the first method to conclude that 7 divides 413 since 7 divides $41 + 5 \cdot 3 = 56$.

Divisibility by 8

Theorem

A number, $1000e + f$, where f is the last three digits, is divisible by 8 if and only if the last three digits are divisible by 8.

- Proof: We have

$$1000e + f \equiv f \pmod 8. \quad \square$$

Divisibility by 11 1

Theorem

A number, $10a + b = \sum_{i=0}^{n} a_i(1{,}000)^i$*, where b is the last digit and the* a_i*'s are blocks of digits of length three starting from the right, is divisible by 11 if and only if 11 divides* $a - b$ *or* $\sum_{i=0}^{n}(-1)^i a_i$*.*

$$11 | 10a + b \Leftrightarrow 11 | a - b, \tag{1}$$

$$11 | \sum_{i=0}^{n} a_i(1{,}000)^i \Leftrightarrow 11 | \sum_{i=0}^{n}(-1)^i a_i. \tag{2}$$

Divisibility by 11 2

- Proof: We have $10 \equiv -1 \pmod{11}$, so

$$10a + b \equiv -a + b \equiv (-1)(a - b) \pmod{11},$$

which is 0 if and only if $a - b \equiv 0 \pmod{11}$

- The second part follows from $10^3 \equiv (-1)^3 \equiv -1 \pmod{11}$, which gives

$$\sum_{i=0}^{n} a_i (1{,}000)^i \equiv \sum_{i=0}^{n} a_i (-1)^i \pmod{11}. \quad \square$$

Divisibility by 11 3

- $$13{,}580{,}237 = 10 \cdot 1{,}358{,}023 + 7 = 13 \cdot 10^6 + 580 \cdot 10^3 + 237 \cdot 10^0.$$

- $$\begin{aligned} 1{,}358{,}023 - 7 &= 1{,}358{,}016, \\ 135{,}801 - 6 &= 135{,}795, \\ 13{,}579 - 5 &= 13{,}574, \\ 1357 - 4 &= 1353, \\ 135 - 3 &= 132, \\ 13 - 2 &= 11, \end{aligned}$$

  so 11 divides 13,580,237.

Divisibility by 11 4

- $$13{,}580{,}237 \equiv 13 - 580 + 237 \equiv -330 \pmod{11},$$

  and 11 divides -330 so so 11 divides 13,580,237.

Divisibility by 13 1

Theorem

A number, $10a + b = 100c + d = \sum_{i=0}^{n} a_i 10^{3i}$, where b is the last digit, d is the last two digits, and the a_i's are blocks of digits of length three starting from the right, is divisible by 13 if and only if 13 divides $a + 4b$, $4c - d$ or $\sum_{i=0}^{n}(-1)^i a_i$.

$$13|10a + b \Leftrightarrow 13|a + 4b, \tag{3}$$

$$13|100c + d \Leftrightarrow 13|4c - d, \tag{4}$$

$$13|\sum_{i=0}^{n} a_i (1{,}000)^i \Leftrightarrow 13|\sum_{i=0}^{n}(-1)^i a_i. \tag{5}$$

Divisibility by 13 2

- Proof: We have

$$10a + b \equiv 10a + 40b \equiv 10(a + 4b) \pmod{13},$$

which is 0 if and only if $a + 4b \equiv 0 \pmod{13}$, since 10 is invertible in $\mathbb{Z}_{13}$.

- The second part follows from

$$100c + d \equiv (104 - 4)c + d \equiv d - 4c \pmod{13}.$$

- The last part follows from $10^3 \equiv (-3)^3 \equiv -27 \equiv -1 \pmod{13}$, which gives

$$\sum_{i=0}^{n} a_i (1{,}000)^i \equiv \sum_{i=0}^{n} (-1)^i a_i \pmod{13}. \qquad \square$$

The Legends of the Condor Heroes 1

- As an another application of modular arithmetic, we will show how we can solve one of the mathematical problems in the Chinese novel Legends of the Condor Heroes (射鵰英雄傳, Shèdiāo yīngxióng zhuàn) by JĪN Yōng 金庸.
- The heroine HUÁNG Róng (黃蓉) is angry at The Divine Mathematician Yīnggū (神算子瑛姑), so she gives her three problems that she thinks Yīnggū will not be able to solve.

The Legends of the Condor Heroes 2

- One of the problems is an example from The Mathematical Classic of Master Sun (孫子算經, Sūnzǐ suànjīng), which was written during the 3rd to 5th centuries CE. It is also known as the Ghost Valley Mathematics Problem (鬼谷算题 Guǐgǔ suàntí).
- "There is an unknown number; three and three has two as the remainder, five and five has three as the remainder, seven and seven has two as the remainder, what mathematical operand is that? Author's note: this problem belongs to the theory of numbers of higher mathematics; our Song Dynasty scholars have been quite profound in this kind of study."

The Legends of the Condor Heroes 3

- We need to solve the equations

$$\begin{aligned} n &\equiv 2 \pmod{3} \\ n &\equiv 3 \pmod{5} \\ n &\equiv 2 \pmod{7} \end{aligned}$$

- There is a method called the Chinese Remainder Theorem that gives an algorithm for solving this kind of problems. We will first find numbers n_1, n_2 and n_3 such that

$$\begin{aligned} n_1 &\equiv 1 \pmod{3} \\ n_1 &\equiv 0 \pmod{35} \\ n_2 &\equiv 1 \pmod{5} \\ n_2 &\equiv 0 \pmod{21} \\ n_3 &\equiv 1 \pmod{7} \\ n_3 &\equiv 0 \pmod{15} \end{aligned}$$

The Legends of the Condor Heroes 4

- We can then find a solution by setting

$$n = 2n_2 + 3n_2 + 2n_3$$

- The reason why we can find the n_i is that 3, 5 and 7 do not have any common factors. Therefore $\gcd(3, 5 \cdot 7) = 1$, and we can find a and b such that $3a + 35b = 1$. We can then set $n_1 = 35b$.
- To find a and b we use the Euclidean algorithm.

$$\begin{aligned}\gcd(35,3) &= (35 - 11 \cdot 3, 3) = (2,3) = (2, 3 - 2 \cdot 1) \\ &= (2,1) = (2 - 2 \cdot 1, 1) = (0,1),\end{aligned}$$

and then run it backwards to get

$$1 = 3 - 2 = 3 - (35 - 11 \cdot 3) = 12 \cdot 3 - 35.$$

- It follows that we can set $n_1 = -35$. However, since our solution n is only determined up to multiples of $3 \cdot 5 \cdot 7 = 105$, we can instead set $n_1 = 105 - 35 = 70$.

The Legends of the Condor Heroes 5

- In the same way we can find $n_2 = 21$ and $n_3 = 15$, which gives us $n = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233$ as a solution, but if we want to get a number between 0 and 104, we can use $23 \equiv 233 - 2 \cdot 105$.

Fermat's Little Theorem 1

Theorem (Fermat's Little Theorem)

Let p be a prime number. If $\gcd(p, a) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

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

$$a \cdot i \equiv a \cdot j \pmod{p},$$
$$a(i-j) \equiv 0 \pmod{p}$$

and since $p \not| a$, 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 $(p-1)! \not\equiv 0 \pmod{p}$. $\square$

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 the 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 the the factors must be divisible by 3.

Euler's ϕ function 1

- In 1763, Leonhard Euler (1707–1783) defined $\phi(n)$ to be the number of integers k with $1 \leq k \leq n$ that are coprime with n.
- If p is prime and $1 \leq k \leq p$, then $\gcd(k, p) = 1$ unless $k = p$, since $\gcd(p, p) = p$.
- It follows that

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

  for any prime number p.
- Notice, however, that $\phi(1) = 1$, since 1 is the only number that is coprime with itself.

Euler's ϕ function 2

- For powers of a prime, we see that the only numbers less than or equal to p^k that have a common factor greater than 1 with p^k are the multiples of p, i.e., xp for $1 \leq x \leq p^{k-1}$. This gives us

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

- $\phi(4) = \phi(2^2) = 4 - 2 = 2.$
- $\phi(8) = \phi(2^3) = 8 - 4 = 4.$

Euler's ϕ function 3

- To compute $\phi(pq)$ for the product of two distinct primes, p and q, we will first give an example and consider $p = 5$ and $q = 7$. The only numbers less than or equal to 35 that are not coprime with 35 are the multiples of 5 and 7. There are 7 multiples of 5 and 5 multiples of 7 less than or equal to 35, i.e. 5, 10, 15, 20, 25, 30, 35 and 7, 14, 21, 28, 35. Notice that the only number in this list that is a multiple of both 5 and 7 is 35, since $\text{lcm}(5,7) = 5 \cdot 7/\gcd(5,7) = 35/1 = 35$.
- We have therefore only counted one number twice, namely 35.
- It follows that $\phi(35) = 35 - 7 - 5 + 1 = 24 = 4 \cdot 6 = \phi(5)\phi(7)$

Euler's ϕ function 4

- For the general case we start with the pq numbers from 1 to pq and subtract the q multiples of p and the p multiples of q. Since $\mathrm{lcm}(p, q) = pq/\gcd(p, q) = pq$, the only number that is subtracted twice is pq. It follows that

$$\phi(pq) = pq - q - p + 1 = (p-1)(q-1) = \phi(p)\phi(q).$$

- Notice that this can also be written as

$$\phi(pq) = (p-1)(q-1) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

Euler's ϕ function 5

- To compute $\phi(p^a q^b)$ for the product of powers of two distinct primes, p and q, we again start with the $p^a q^b$ numbers from 1 to $p^a q^b$ and subtract the $p^{a-1}q$ multiples of p and the pq^{b-1} multiples of q. However, this time multiples of pq are counted twice so we must add the $p^{a-1}q^{b-1}$ multiples of pq to get

$$
\begin{aligned}
\phi(p^a q^b) &= p^a q^b - p^{a-1} q^b - p^a q^{b-1} + p^{a-1} q^{b-1} \\
&= p^a q^b - p^a q^b / p - p^a q^b / q + p^a q^b / (pq) \\
&= p^a q^b (1 - 1/p - 1/q + 1/(pq)) \\
&= p^a q^b (1 - 1/p)(1 - 1/q) = \phi(p)\phi(q).
\end{aligned}
$$

Euler's ϕ function 6

- To compute $\phi(p^a q^b r^c)$ for the product of powers of three distinct primes, p, q and r, we start in the same way, but now multiples of pq, pr and qr that are not multiples of pqr are all counted twice so we must add these multiples.
- However, multiples of pqr are first subtracted three times (multiples of p, q and r) and then added three times (multiples of pq, pr and qr), so we must subtract them. This gives us

$$
\begin{gathered}
\phi(p^a q^b r^c) = p^a q^b r^c - p^a q^b r^c/p - p^a q^b r^c/q - p^a q^b r^c/r \\
+ p^a q^b r^c/(pq) + p^a q^b r^c/(pr) + p^a q^b r^c/(qr) - p^a q^b r^c/(pqr) \\
= p^a q^b r^c(1 - 1/p - 1/q - 1/r + 1/(pq) + 1/(pr) + 1/(qr) \\
-1/(pqr) = p^a q^b r^c(1 - 1/p)(1 - 1/q)(1 - 1/r).
\end{gathered}
$$

Euler's ϕ function 7

- Using similar arguments, we can show that

$$\phi\left(\prod_{i=1}^{r} p_i^{a_i}\right) = \prod_{i=1}^{r} p_i^{a_i}\left(1 - \frac{1}{p_i}\right).$$

- This can also be written as

$$\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right),$$

  where the product is over all the prime factors in n.

- Notice also that this formula shows that ϕ is multiplicative in the sense that

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

- So $\phi(12) = \phi(4)\phi(3) = (4-2)2 = 4$, while $\phi(2)\phi(6) = 1 \cdot (3-1)(2-1) = 2$.

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 $\gcd(c, n) = 1$. $\square$

Euler's Theorem 2

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

Order of an element

- If $\overline{a} \in \mathbb{Z}_n$ is invertible, 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 of* a*, then* $k | \phi(n)$*.*

- Proof: We know that $a^{\phi(n)} \equiv 1 \pmod{n}$. If we divide $\phi(n)$ by k, we get $\phi(n) = lk + r$, where $0 \leq r < k$, and then

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

  Since k is smallest positive number with $a^k \equiv 1 \pmod{n}$, we must have $r = 0$, so $k | \phi(n)$. $\square$
- In $\mathbb{Z}_5$, the orders of $\overline{2}$ and $\overline{3}$ are $\phi(5) = 4$, but the order of $\overline{4}$ is 2.
- In $\mathbb{Z}_6$, the order of $\overline{5}$ is $\phi(6) = 2$.
- In $\mathbb{Z}_8$, the orders of $\overline{3}$, $\overline{5}$ and $\overline{7}$ are $2 = \phi(8)/2$.