Number Theory

ITT9132 Concrete Mathematics

Contents

Next section

Congruences

Definition

Let $a, b, c \in \mathbb{Z}$ with $m \geqslant 1$. a is congruent to b modulo m, written $a \equiv b \pmod{m}$, if a and b give the same remainder when divided by m.

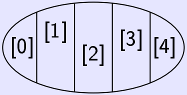
Alternative definition: $a \equiv b \pmod{m}$ iff $m \backslash (b-a)$.

Congruence is an equivalence relation:

Reflexivity: $a \equiv a \pmod{m}$.

Symmetry: if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

Transitivity: if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.



Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d \setminus m$, then $a \equiv b \pmod{d}$.
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{\operatorname{lcm}(m_1, m_2, \ldots, m_k)}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$ for any integer c.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$.
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = 1$, then $a \equiv b \pmod{m}$.
- $a \equiv b \pmod{m}$ if and only if $ak \equiv bk \pmod{mk}$ for every natural number k.

Warmup: An impossible Josephus problem

The problem

Ten people are sitting in circle, and every *m*th person is executed.
Prove that, for every $k \geqslant 1$, the first, second, and third person executed *cannot* be 10, k, and $k+1$, in this order.

Warmup: An impossible Josephus problem

The problem

Ten people are sitting in circle, and every mth person is executed.
Prove that, for every $k \geqslant 1$, the first, second, and third person executed *cannot* be 10, k, and $k+1$, in this order.

Solution

- If 10 is the first to be executed, then $10|m$.
- If k is the second to be executed, then $m \equiv k \pmod 9$.
- If $k+1$ is the third to be executed, then $m \equiv 1 \pmod 8$, because $k+1$ is the first one after k.

But if $10|m$, then m is even, and if $m \equiv 1 \pmod 8$, then m is odd: it cannot be both at the same time.

Application of congruence relation

Example 1: Find the remainder of the division of $a = 1395^4 \cdot 675^3 + 12 \cdot 17 \cdot 22$ by 7.

As $1395 \equiv 2 \pmod 7$, $675 \equiv 3 \pmod 7$, $12 \equiv 5 \pmod 7$, $17 \equiv 3 \pmod 7$ and $22 \equiv 1 \pmod 7$, we have:

$$a \equiv 2^4 \cdot 3^3 + 5 \cdot 3 \cdot 1 \pmod 7$$

As $2^4 = 16 \equiv 2 \pmod 7$, $3^3 = 27 \equiv 6 \pmod 7$, and $5 \cdot 3 \cdot 1 = 15 \equiv 1 \pmod 7$, it follows

$$a \equiv 2 \cdot 6 + 1 = 13 \equiv 6 \pmod 7$$

Application of congruence relation

Example 2: Find the remainder of the division of $a = 53 \cdot 47 \cdot 51 \cdot 43$ by 56.

A. As $53 \cdot 47 = 2491 \equiv 27 \pmod{56}$ and $51 \cdot 43 = 2193 \equiv 9 \pmod{56}$,

$$a \equiv 27 \cdot 9 = 243 \equiv 19 \pmod{56}$$

B. As $53 \equiv -3 \pmod{56}$, $47 \equiv -9 \pmod{56}$, $51 \equiv -5 \pmod{56}$ and $43 \equiv -13 \pmod{56}$,

$$a \equiv (-3) \cdot (-9) \cdot (-5) \cdot (-13) = 1755 \equiv 19 \pmod{56}$$

Application of congruence relation

Example 3: Find the remainder of the division of 45^{69} by 89

We make use of the method of squares:

$$\begin{aligned}
45 &\equiv 45 \pmod{89} \\
45^2 &= 2025 \equiv 67 \pmod{89} \\
45^4 &= (45^2)^2 \equiv 67^2 = 4489 \equiv 39 \pmod{89} \\
45^8 &= (45^4)^2 \equiv 39^2 = 1521 \equiv 8 \pmod{89} \\
45^{16} &= (45^8)^2 \equiv 8^2 = 64 \equiv 64 \pmod{89} \\
45^{32} &= (45^{16})^2 \equiv 64^2 = 4096 \equiv 2 \pmod{89} \\
45^{64} &= (45^{32})^2 \equiv 2^2 = 4 \equiv 4 \pmod{89}
\end{aligned}$$

As $69 = 64 + 4 + 1$,

$$45^{69} = 45^{64} \cdot 45^4 \cdot 45^1 \equiv 4 \cdot 39 \cdot 45 \equiv 7020 \equiv 78 \pmod{89}$$

Application of congruence relation

Let $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$, where $a_i \in \{0, 1, \ldots, 9\}$ are digits of its decimal representation.

Theorem

An integer n is divisible by 11 iff the difference of the sums of the odd-numbered digits and the even-numbered digits is divisible by 11:

$$11 | (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots)$$

Proof:

- We observe that $10 \equiv -1 \pmod{11}$.
- Then, $10^i \equiv (-1)^i \pmod{11}$ for every i.
- We can conclude:

$$\begin{aligned} n &= a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \\ &\equiv a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \ldots + a_1 \cdot (-1) + a_0 \\ &\equiv (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) \pmod{11} \text{Q.E.D.`} \end{aligned}$$

Example 4: 34425730438 is divisible by 11

Indeed: $8 + 4 + 3 + 5 + 4 + 3 = 27$ and $3 + 0 + 7 + 2 + 4 = 16$, with $27 - 16 = 11$.

Attention to the powers!

Replacing numbers with congruence classes does not work with exponents!

- Let $n = 7$, $a = 11$, and $e = 17$.
- Then $a \equiv 4 \pmod{n}$ and $e \equiv 3 \pmod{n}3$.
- Now, $4^3 = 64 = 9 \cdot 7 + 1$, so $(11 \bmod 7)^{17 \bmod 7} \equiv 1 \pmod{7}$.
- However, $11^{17} \equiv 2 \pmod{7}$, because $11^{17} = 505447028499293771 = 72206718357041967 \cdot 7 + 2$.

Attention to the powers!

Replacing numbers with congruence classes does not work with exponents!

- Let $n = 7$, $a = 11$, and $e = 17$.
- Then $a \equiv 4 \pmod{n}$ and $e \equiv 3 \pmod{n}3$.
- Now, $4^3 = 64 = 9 \cdot 7 + 1$, so $(11 \bmod 7)^{17 \bmod 7} \equiv 1 \pmod{7}$.
- However, $11^{17} \equiv 2 \pmod{7}$, because $11^{17} = 505447028499293771 = 72206718357041967 \cdot 7 + 2$.

Reason why:

- Among integers, exponentiation is not a basic operation:
- Instead, it is the result of a sequence of multiplications.
- If you change the number of factors of a multiplication you cannot, in general, be sure that the result will stay the same.

Attention to the powers!

Replacing numbers with congruence classes does not work with exponents!

- Let $n = 7$, $a = 11$, and $e = 17$.
- Then $a \equiv 4 \pmod{n}$ and $e \equiv 3 \pmod{n}3$.
- Now, $4^3 = 64 = 9 \cdot 7 + 1$, so $(11 \bmod 7)^{17 \bmod 7} \equiv 1 \pmod{7}$.
- However, $11^{17} \equiv 2 \pmod{7}$, because $11^{17} = 505447028499293771 = 72206718357041967 \cdot 7 + 2$.

Reason why:

- Among integers, exponentiation is not a basic operation:
- Instead, it is the result of a sequence of multiplications.
- If you change the number of factors of a multiplication you cannot, in general, be sure that the result will stay the same.

Solution: use Fermat's little theorem and/or Euler's theorem.

Strange numbers: "arithmetic of days of the week"

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Strange numbers: "arithmetic of days of the week"

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Commutativity:

$$Tu + Fr = Fr + Tu \qquad Tu \cdot Fr = Fr \cdot Tu$$

Strange numbers: "arithmetic of days of the week"

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Associativity:

$$(Mo + We) + Fr = Mo + (We + Fr) \qquad (Mo \cdot We) \cdot Fr = Mo \cdot (We \cdot Fr)$$

Strange numbers: "arithmetic of days of the week"

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Subtraction is the inverse operation of addition:

$$Th - We = (Mo + We) - We = Mo$$

Strange numbers: "arithmetic of days of the week"

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Su is the zero element:

$$We + Su = We \qquad\qquad We \cdot Su = Su$$

Strange numbers: "arithmetic of days of the week"

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Mo is the unit:

$$We \cdot Mo = We$$

Arithmetics modulo m

- Numbers are denoted by $\overline{0}, \overline{1}, \ldots, \overline{m-1}$, where $\overline{a}$ represents the class of all integers that, divided by m, give remainder a.
- Operations are defined as follows:

$$\overline{a} + \overline{b} = \overline{c} \text{ iff } a + b \equiv c \pmod{m}$$
$$\overline{a} \cdot \overline{b} = \overline{c} \text{ iff } a \cdot b \equiv c \pmod{m}$$

Examples

- "arithmetic of days of the week", with modulus 7.
- Boolean algebra, with modulus 2.

Division in modular arithmetic

- Dividing $\overline{a}$ by $\overline{b}$ means to find a quotient x, such that $\overline{b} \cdot x = \overline{a}$, that is, $\overline{a}/\overline{b} = x$

In "arithmetic of days of the week":

- $Mo/Tu = Th$ and $Tu/Mo = Tu$.
- We cannot divide by Su, exceptionally Su/Su could be any day.
- A quotient is well defined for $\overline{a}/\overline{b}$ for every $\overline{b} \neq \overline{0}$, if the modulus is a prime number.

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Division in modular arithmetic

- Dividing $\overline{a}$ by $\overline{b}$ means to find a quotient x, such that $\overline{b} \cdot x = \overline{a}$, that is, $\overline{a}/\overline{b} = x$

In "arithmetic of days of the week":

- $Mo/Tu = Th$ and $Tu/Mo = Tu$.
- We cannot divide by Su, exceptionally Su/Su could be any day.
- A quotient is well defined for $\overline{a}/\overline{b}$ for every $\overline{b} \neq \overline{0}$, if the modulus is a prime number.

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Division in modular arithmetic

- Dividing $\overline{a}$ by $\overline{b}$ means to find a quotient x, such that $\overline{b} \cdot x = \overline{a}$, that is, $\overline{a}/\overline{b} = x$

In "arithmetic of days of the week":

- $Mo/Tu = Th$ and $Tu/Mo = Tu$.
- We cannot divide by Su, exceptionally Su/Su could be any day.
- A quotient is well defined for $\overline{a}/\overline{b}$ for every $\overline{b} \neq \overline{0}$, if the modulus is a prime number.

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Division in modular arithmetic

- Dividing $\overline{a}$ by $\overline{b}$ means to find a quotient x, such that $\overline{b} \cdot x = \overline{a}$, that is, $\overline{a}/\overline{b} = x$

In "arithmetic of days of the week":

- $Mo/Tu = Th$ and $Tu/Mo = Tu$.
- We cannot divide by Su, exceptionally Su/Su could be any day.
- A quotient is well defined for $\overline{a}/\overline{b}$ for every $\overline{b} \neq \overline{0}$, if the modulus is a prime number.

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Division modulo a prime p

Theorem

If x and m are positive integers and $\gcd(x,m) = 1$, then the numbers

$$\overline{x} \cdot \overline{0}, \overline{x} \cdot \overline{1}, \ldots, \overline{x} \cdot \overline{m-1}$$

are pairwise different.

Proof:

- Suppose $0 \leqslant i \leqslant j < m$ are such that $x \cdot i \equiv x \cdot j \pmod{m}$.
- Then $m \backslash x \cdot (j-i)$: as $\gcd(m,x) = 1$, it must be $m \backslash j - i$.
- But $j - i < m$, so it must be $j - i = 0$, that is, $i = j$. Q.E.D.

Corollary

If m is prime, then the quotient $\overline{x} = \overline{a}/\overline{b}$ of the division of $\overline{a}$ by $\overline{b}$ modulo m is well defined for every $\overline{b} \neq \overline{0}$.

If the modulus is not prime ...

The quotient is not well defined, for example:

$$\overline{1} = \overline{2}/\overline{2} = \overline{3}$$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Computing $\overline{x} = \overline{a}/\overline{b}$ modulo a prime p

In two steps:

1. Compute $\overline{y} = \overline{1}/\overline{b}$.
2. Compute $\overline{x} = \overline{y} \cdot \overline{a}$.

How to compute $\overline{y} = \overline{1}/\overline{b}$, i.e. find $\overline{y}$ such that $\overline{b} \cdot \overline{y} = \overline{1}$
Algorithm:

1. Using the Euclidean algorithm, compute $\gcd(p, b) = 1$.
2. Find coefficients s and t such that $ps + bt = 1$
3. **if** $t \geqslant p$ **then**
   $t \leftarrow t$ **mod** p
   endif
4. **return** t % Property: $\overline{t} = \overline{1}/\overline{b}$

Division modulo p

Example: compute $\overline{53}/\overline{2}$ modulo 234527

- At first, we find $\overline{1}/\overline{2}$. For that we compute GCD of the divisor and modulus:

$$\gcd(234527, 2) = \gcd(2, 1) = 1$$

- The remainder can be expressed by modulus ad divisor as follows:

$$1 = 2 \cdot (-117263) + 234527 \text{ or}$$
$$-117263 \cdot 2 \equiv 117264 \pmod{234527}$$

Thus, $\overline{1}/\overline{2} = \overline{117264} \pmod{234527}$

- As $x = 53 \cdot 117264 \equiv 117290 \pmod{234527}$, we conclude:

$$\overline{x} = \overline{53} \cdot \overline{117264} = \overline{117290} \pmod{234527}.$$

Linear equations

Solve the equation $\overline{7}\overline{x}+\overline{3}=\overline{0}$ modulo 47

The solution can be written as $\overline{x}=-\overline{3}/\overline{7}$.

- Compute $\gcd(47,7)$ using the Euclidean algorithm:

$$\gcd(47,7)=\gcd(7,5)=\gcd(5,2)=\gcd(2,1)=1$$

  that yields the relations

$$1=5-2\cdot 2 \qquad 2=7-5 \qquad 5=47-6\cdot 7$$

- Find coefficients of 47 and 7:

$$\begin{aligned}1 &= 5-2\cdot 2= \\ &= (47-6\cdot 7)-2\cdot(7-5)= \\ &= 47-8\cdot 7+2\cdot 5= \\ &= 47-8\cdot 7+2\cdot(47-6\cdot 7)= \\ &= 3\cdot 47-20\cdot 7\end{aligned}$$

Continues on the next slide ...

Linear equations (2)

Solve the equation $\overline{7}\overline{x} + \overline{3} = \overline{0}$modulo 47

- The previous expansion of gcd(47,7) shows that $-20 \cdot 7 \equiv 1 \pmod{47}$ i.e. $27 \cdot 7 \equiv 1 \pmod{47}$
  Hence, $\overline{1}/\overline{7} = \overline{-20} = \overline{27} \pmod{47}$.
- The solution is then: $\overline{x} = \overline{-3} \cdot \overline{27} = \overline{13}$.

The latter equality follows from the congruence relation $44 \equiv -3 \pmod{47}$, whence $x = 44 \cdot 27 = 1188 \equiv 13 \pmod{47}$.

Solving a system of equations using the elimination method

Example

Assuming modulus 127, find integers x and y such that:

$$\begin{cases} \overline{12}\overline{x}+\overline{31}\overline{y}=\overline{2} \\ \overline{2}\overline{x}+\overline{89}\overline{y}=\overline{23} \end{cases}$$

Accordingly to the elimination method, multiply the second equation by $-\overline{6}$ and add up the equations, we get:

$$\overline{y}=\frac{\overline{2}-\overline{6}\cdot\overline{23}}{\overline{31}-\overline{6}\cdot\overline{89}}$$

As $6\cdot 23=138\equiv 11 \pmod{127}$ and $6\cdot 89=534\equiv 26 \pmod{127}$, the latter equality can be transformed as follows:

$$\overline{y}=\frac{\overline{2}-\overline{11}}{\overline{31}-\overline{26}}=\frac{-\overline{9}}{\overline{5}}$$

Substituting $\overline{y}$ into the second equation, express $\overline{x}$ and transform it further considering that $5\cdot 23=115\equiv -12 \pmod{127}$ and $9\cdot 89=801\equiv 39 \pmod{127}$:

$$\overline{x}=\frac{\overline{23}-\overline{89}\overline{y}}{\overline{2}}=\frac{\overline{23}\cdot\overline{5}-\overline{899}}{\overline{10}}=\frac{\overline{-12}+\overline{39}}{\overline{10}}=\frac{\overline{27}}{\overline{10}}$$

Solving a system of equations using elimination method (2)

Continuation of the last example ...

Computing:

$$\begin{cases} \overline{x} = \overline{27}/\overline{10} \\ \overline{y} = -\overline{9}/\overline{5} \end{cases}$$

if the modulus is 127.

Apply the Euclidean algorithm:

$$\gcd(127,5) = \gcd(5,2) = \gcd(2,1) = 1$$
$$\gcd(127,10) = \gcd(10,7) = \gcd(7,3) = \gcd(3,1) = 1$$

That gives the equalities:

$$1 = 5 - 2\cdot 2 = 5 - 2(127 - 25\cdot 5) = (-2)127 + 51\cdot 5$$
$$1 = 7 - 2\cdot 3 = 127 - 12\cdot 10 - 2(10 - 127 + 12\cdot 10) = 3\cdot 127 - 38\cdot 10$$

Hence, division by $\overline{5}$ is equivalent to multiplication by $\overline{51}$ and division by $\overline{10}$ to multiplication to $-\overline{38}$. Then the solution of the system is:

$$\begin{cases} \overline{x} = \overline{27}/\overline{10} = -\overline{27}\cdot\overline{38} = -\overline{1026} = \overline{117} \\ \overline{y} = -\overline{9}/\overline{5} = -\overline{9}\cdot\overline{51} = -\overline{459} = \overline{49} \end{cases}$$

Next section

To determine whether a number n is prime.

Options available:

- Try all numbers $2, \dots, n-1$. If n is not divisible by any of them, then it is prime.
- Same as above, only try $2, \dots, \sqrt{n}$. Exercise: why?
- Probabilistic algorithms with polynomial complexity (Fermat's test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal, Kayal and Saxena (2002).

Next subsection

Fermat's Little Theorem: Statement

Fermat's Little Theorem

If p is prime and a is an integer not divisible by p, then

$$p \setminus a^{p-1} - 1\,, \text{ that is}\,, \; a^{p-1} \equiv 1 \pmod{p}\,.$$

Pierre de Fermat (1601–1665)

Fermat's Little Theorem: Statement

Fermat's Little Theorem

If p is prime and a is an integer not divisible by p, then

$$p \setminus a^{p-1} - 1\,, \ \text{that is}\,, \ a^{p-1} \equiv 1 \pmod{p}\,.$$

The following lemma will be useful for the proof of FLT:

Lemma

If p is prime and $0 < k < p$, then $p \setminus \binom{p}{k}$

Proof:

- Clearly, $\binom{p}{k} = \frac{p^{\underline{k}}}{k!} = \frac{p \cdot (p-1)^{\underline{k-1}}}{k!}$ whenever $0 < k < p$.
- Then p appears once in the numerator, and never in the denominator.

Pierre de Fermat (1601–1665)

Another formulation of the theorem

Fermat's Little Theorem (equivalent statement)

If p is prime, and a is *any* integer, then

$$p \setminus a^p - a\,, \text{ that is}\,, \; a^p \equiv a \pmod{p}\,.$$

Proof by induction on $a \geqslant 0$ with arbitrary p:

- If $p \setminus a$ then $p \setminus a^p$ too, and both a and a^p are congruent to 0 modulo p. In particular, FLT is true for $a = 0$.
- Suppose then that FLT is true for $a \geqslant 0$. Then by the binomial theorem:

$$\begin{aligned}
(a+1)^p - (a+1) &= \sum_{k=0}^{p} \binom{p}{k} a^{p-k} - a - 1 \\
&= (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}
\end{aligned}$$

  Each summand on the last line is divisible by p, the first one by induction, the others by the lemma. Then FLT is also true for $a+1$.

Application of the Fermat's theorem

Example: Find the remainder of the division of 3^{4565} by 13.

Fermat's little theorem gives $3^{12} \equiv 1 \pmod{13}$. Let's divide 4565 by 12 and compute the remainder: $4565 = 380 \cdot 12 + 5$. Then:

$$3^{4565} = (3^{12})^{380} \cdot 3^5 \equiv 1^{380} \cdot 3^5 = 81 \cdot 3 \equiv 3 \cdot 3 = 9 \pmod{13}$$

Application of Fermat's theorem (2)

Prove that $n^{18}+n^{17}-n^2-n$ is divisible by 51 for any positive integer n.

Let's factorize:

$$\begin{aligned}
A &= n^{18}+n^{17}-n^2-n \\
&= n(n^{17}-n)+n^{17}-n \\
&= (n+1)(n^{17}-n) \\
&= (n+1)n(n^{16}-1) \\
&= (n+1)n(n^8-1)(n^8+1) \\
&= (n+1)n(n^4-1)(n^4+1)(n^8+1) \\
&= (n+1)n(n^2-1)(n^2+1)(n^4+1)(n^8+1) \\
&= (n+1)n(n-1)(n+1)(n^2+1)(n^4+1)(n^8+1)
\end{aligned}$$

By the third line, A is divisible by 17; by the last line, A is divisible by 3. Hence, A is divisible by $17\cdot 3=51$.

Pseudoprimes

A pseudoprime is a composite number which has some properties also satisfied by all prime numbers.

- The thesis of FLT is also true for some composite numbers.
- For instance, if $p = 341 = 11 \cdot 31$ and $a = 2$, then dividing

  $$2^{340} = (2^{10})^{34} = 1024^{34}$$

  by 341 yields the remainder 1, because $341 \cdot 3 = 1023$.
- The integer 341 is a Fermat pseudoprime for base 2.
- However, 341 *is not* a Fermat pseudoprime for base 3, because the thesis of FLT is not satisfied for $a = 341$ and $p = 3$: dividing 3^{340} by 341 gives remainder 56.

Carmichael numbers

Definition

A Carmichael number is an integer n that is a Fermat pseudoprime for every base a coprime to n.

Example: let $n = 561 = 3 \cdot 11 \cdot 17$ and $\gcd(a, n) = 1$.

$$a^{560} = (a^2)^{280} \text{ gives remainder 1 if divided by 3}$$
$$a^{560} = (a^{10})^{56} \text{ gives remainder 1 if divided by 11}$$
$$a^{560} = (a^{16})^{35} \text{ gives remainder 1 if divided by 17}$$

Hence, $a^{560} - 1$ is divisible by 3, by 11 and by 17—thus also by 561.

- See `http://oeis.org/search?q=Carmichael`, sequence nr A002997

Next subsection

Fermat's test

Fermat's theorem: If p is prime and $1 \leqslant a < p$ is integer, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

To test, whether n is prime or composite:

- Check if $a^{n-1} \equiv 1 \pmod{n}$ for every $a = 2, 3, \ldots, n-1$.
- If the condtion is not satisfied for some a, then n is composite.
- Otherwise, *n might be* prime.

Example: is 221 prime?

$$2^{220} = \left(2^{11}\right)^{20} \equiv 59^{20} = \left(59^4\right)^5 \equiv 152^5 =$$
$$= 152 \cdot \left(152^2\right)^2 \equiv 152 \cdot 120^2 \equiv 152 \cdot 35 = 5320 \equiv 16 \pmod{221}$$

Hence, 221 is a composite number. Indeed, $221 = 13 \cdot 17$

Fermat's test

Fermat's theorem: If p is prime and $1 \leqslant a < p$ is integer, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

To test, whether n is prime or composite:

- Check if $a^{n-1} \equiv 1 \pmod{n}$ for every $a = 2, 3, \ldots, n-1$.
- If the condtion is not satisfied for some a, then n is composite.
- Otherwise, n *might be* prime.

Example: is 221 prime?

$$\begin{aligned} 2^{220} &= \left(2^{11}\right)^{20} \equiv 59^{20} = \left(59^4\right)^5 \equiv 152^5 = \\ &= 152 \cdot \left(152^2\right)^2 \equiv 152 \cdot 120^2 \equiv 152 \cdot 35 = 5320 \equiv 16 \pmod{221} \end{aligned}$$

Hence, 221 is a composite number. Indeed, $221 = 13 \cdot 17$

Problems with Fermat's test

- Computing of large powers is problematic.
  Possible solution: method of squares for fast exponentiation.
- Computing with large numbers in general is expensive.
  Possible turnaround: modular arithmetic.
- n might be a pseudoprime.
  Possible solution: repeat the test for many randomly chosen values of a.
- n might be a Carmichael number.
  Solutions: use another method!, for example, the Rabin-Miller test.

Problems with Fermat's test

- Computing of large powers is problematic.
  Possible solution: method of squares for fast exponentiation.
- Computing with large numbers in general is expensive.
  Possible turnaround: modular arithmetic.
- n might be a pseudoprime.
  Possible solution: repeat the test for many randomly chosen values of a.
- n might be a Carmichael number.
  Solutions: use another method!, for example, the Rabin-Miller test.

Problems with Fermat's test

- Computing of large powers is problematic.
  Possible solution: method of squares for fast exponentiation.
- Computing with large numbers in general is expensive.
  Possible turnaround: modular arithmetic.
- n might be a pseudoprime.
  Possible solution: repeat the test for many randomly chosen values of a.
- n might be a Carmichael number.
  Solutions: use another method!, for example, the Rabin-Miller test.

Problems with Fermat's test

- Computing of large powers is problematic.
  Possible solution: method of squares for fast exponentiation.
- Computing with large numbers in general is expensive.
  Possible turnaround: modular arithmetic.
- n might be a pseudoprime.
  Possible solution: repeat the test for many randomly chosen values of a.
- n might be a Carmichael number.
  Solutions: use another method!, for example, the Rabin-Miller test.

Modified Fermat's test

Input: n – a value to test for primality
k – the number of times to test for primality
Output: "n is composite" or "n is probably prime".

- **for** i **in** $[1:k]$ **do**
  - pick a random $1 < a < n$
  - **if** $a^{n-1} \not\equiv 1 \pmod{n}$ **then**
    return("n is composite")
    endif

  done
- **return**("n is probably prime")

Modified Fermat's test

Input: n – a value to test for primality
k – the number of times to test for primality
Output: "n is composite" or "n is probably prime".

- **for** i **in** $[1:k]$ **do**
  - pick a random $1 < a < n$
  - **if** $a^{n-1} \not\equiv 1 \pmod{n}$ **then**
    return("n is composite")
    endif

  done
- **return**("n is probably prime")

Example, $n = 221$, randomly picked values for a are 38 and 26

$$a^{n-1} = 38^{220} \equiv 1 \pmod{221} \quad \rightsquigarrow 38 \text{ is pseudoprime}$$

$$a^{n-1} = 26^{220} \equiv 169 \not\equiv 1 \pmod{221} \quad \rightsquigarrow 221 \text{ is composite}$$

Modified Fermat's test

Input: n – a value to test for primality
k – the number of times to test for primality
Output: "n is composite" or "n is probably prime".

- **for** i **in** $[1:k]$ **do**
  - pick a random $1 < a < n$
  - **if** $a^{n-1} \not\equiv 1 \pmod{n}$ **then**
    return("n is composite")
    endif

  done
- **return**("n is probably prime")

Does not work, if n is a Carmichael number: $561, 1105, 1729, 2465, 2821, 6601, 8911, \ldots$

Next subsection

An idea on how to neutralize Carmichael numbers

- Let n be an odd positive integer to be tested for primality.
- Randomly pick an integer a from the interval $0 < a < n$.
- Consider the expression $a^n - a = a(a^{n-1} - 1)$ and until possible, transform it applying the identity $x^2 - 1 = (x-1)(x+1)$.
- If the expression $a^n - a$ is not divisible by n, then none of its divisors is divisible by n either.
- If at least one divisor of $a^n - a$ is divisible by n, then n is probably prime.

The test is made more effective by being repeated many times on randomly chosen values of a.

Example: $n = 221$

- Let's factorize:

$$\begin{aligned} a^{221} - a = a(a^{220} - 1) &= \\ &= a(a^{110} - 1)(a^{110} + 1) = \\ &= a(a^{55} - 1)(a^{55} + 1)(a^{110} + 1) \end{aligned}$$

- If $a = 174$, then
$174^{110} = (174^2)^{55} \equiv (220)^{55} = 220 \cdot (220^2)^{27} \equiv 220 \cdot 1^{27} \equiv 220 \equiv -1 \pmod{221}$.
Thus 221 is either prime or pseudoprime to the base 174.
- If $a = 137$, then $221 \not| a, 221 \not| (a^{55} - 1), 221 \not| (a^{55} + 1), 221 \not| (a^{110} + 1)$.
Consequently, 221 is a composite number

The Rabin-Miller test

Input: $n > 3$ – a value to test for primality
k – the number of times to test for primality
Output: "n is composite" or "n is probably prime"

- Factorize $n - 1 = 2^s \cdot d$, where d is an odd number
- **for** i **in** $[1 : k]$ **do**
  - Randomly pick $a \in [2 : n-1]$
  - $x \leftarrow a^d \bmod n$
  - **if** $x = 1$ **or** $x = n - 1$ **then** % either $n \setminus a^d - 1$ or $n \setminus a^d + 1$
    continue
    endif
  - **for** r **in** $[1 : s-1]$ **do**
    - $x \leftarrow x^2 \bmod n$
    - **if** $x = 1$ **then return**("n is composite") **endif**
    - **if** $x = n - 1$ **then break endif**

    done
  - **return**("n is composite")

  done
- **return**("n is probably prime");

The complexity of the algorithm is $O(k \lg^3 n)$

Next section

Euler's totient function ϕ

Euler's totient function

Euler's totient function ϕ is defined for $m \geqslant 2$ as

$$\phi(m) = |\{n \in \{0, \ldots, m-1\} \mid \gcd(m,n) = 1\}|$$

Equivalently: $\dfrac{\phi(m)}{m}$ is the probability that an integer taken at random between 0 and $m-1$ is relatively prime with m.

m	2	3	4	5	6	7	8	9	10	11	12	13
$\phi(m)$	1	2	2	4	2	6	4	6	4	10	4	12

We can use $[1 : m]$ in place of $[0 : m-1]$ if convenient.

Computing Euler's function

Lemma

1. If $p \geqslant 2$ is prime and $k \geqslant 1$, then $\phi(p^k) = p^k(1 - 1/p) = p^{k-1} \cdot (p-1)$.
2. If $m, n \geqslant 1$ are relatively prime, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Proof

1. Exactly every pth integer n, starting from 0, has $\gcd(p^k, n) \geqslant p > 1$.
   Then $\phi(p^k) = p^k - p^k/p = p^k \cdot (1 - 1/p)$.
2. If $m \perp n$, then for every $k \geqslant 1$ it is $k \perp mn$ if and only if both $m \perp k$ and $n \perp k$.

We have then:

Theorem

$$\phi(m) = m \cdot \prod_{p \text{ prime},\ p \backslash m} \left(1 - \frac{1}{p}\right)$$

Warmup: $\phi(999)$

Problem (Exercise 4.10)

Compute $\phi(999)$.

Warmup: $\phi(999)$

Problem (Exercise 4.10)

Compute $\phi(999)$.

Solution

We factor 999 into a product of primes:

$$999 = 9 \cdot 111 = 9 \cdot 3 \cdot 37 = 3^3 \cdot 37$$

Then:

$$\begin{aligned}
\phi(999) &= 999 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{37}\right) \\
&= 3^3 \cdot 37 \cdot \frac{2}{3} \cdot \frac{36}{37} \\
&= 3^2 \cdot 2 \cdot 2^2 \cdot 3^2 \\
&= 2^3 \cdot 3^4 = 8 \cdot 81 = 648\,.
\end{aligned}$$

Multiplicative functions

Definition

$f : \mathbb{N}^+ \to \mathbb{N}^+$ is multiplicative if it satisfies the following condition:
For every $m, n \geqslant 1$, if $m \perp n$, then $f(m \cdot n) = f(m) \cdot f(n)$

Theorem

If $g(m) = \sum_{d \backslash m} f(d)$ is multiplicative, then so is $f(m)$.

- $g(1) = g(1) \cdot g(1) = f(1)$ must be either 0 or 1.
- If $m = m_1 m_2$ with $m_1 \perp m_2$, then every factor d of $m_1 m_2$ is the product of a factor d_1 of m_1 and a factor d_2 of m_2 in a unique way. Then:

$$\begin{aligned} g(m_1 m_2) &= \sum_{d_1 d_2 \backslash m_1 m_2} f(d_1 d_2) \\ &= \left(\sum_{d_1 \backslash m_1} f(d_1)\right)\left(\sum_{d_2 \backslash m_2} f(d_2)\right) - f(m_1) f(m_2) + f(m_1 m_2) \\ &= g(m_1) g(m_2) - f(m_1) f(m_2) + f(m_1 m_2) \end{aligned}$$

- As $g(m_1 m_2) = g(m_1) g(m_2)$, we conclude: $f(m_1 m_2) = f(m_1) f(m_2)$

$\sum_{d\backslash m}\phi(d) = m$: Example

The fractions

$$\frac{0}{12}, \frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}$$

are simplified into:

$$\frac{0}{1}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{15}{6}, \frac{11}{12}.$$

The divisors of 12 are 1, 2, 3, 4, 6, and 12. Of these:

- The denominator 1 appears $\phi(1) = 1$ time: $0/1$.
- The denominator 2 appears $\phi(2) = 1$ time: $1/2$.
- The denominator 3 appears $\phi(3) = 2$ times: $1/3$, $2/3$.
- The denominator 4 appears $\phi(4) = 2$ times: $1/4$, $3/4$.
- The denominator 6 appears $\phi(6) = 2$ times: $1/6$, $5/6$.
- The denominator 12 appears $\phi(12) = 4$ times: $1/12$, $5/12$, $7/12$, $11/12$.

We have thus found: $\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 12$.

$\sum_{d\backslash m} \phi(d) = m$: Proof

Call a fraction a/b basic if $0 \leqslant a < b$.
After simplifying any of the m basic fractions with denominator m, the denominator d of the resulting fraction must be a divisor of m.

Lemma

In the simplification of the m basic fractions with denominator m, for every divisor d of m, the denominator d appears exactly $\phi(d)$ times.

It follows immediately that $\sum_{d|m} \phi(d) = m$.

Proof

- After simplification, the fraction k/d only appears if $\gcd(k,d) = 1$: for every d there are at most $\phi(d)$ such k.
- But each such k appears in the fraction kh/n, where $h \cdot d = n$.

$\sum_{d\backslash m} \phi(d) = m$: Proof

Call a fraction a/b basic if $0 \leqslant a < b$.
After simplifying any of the m basic fractions with denominator m, the denominator d of the resulting fraction must be a divisor of m.

Lemma

In the simplification of the m basic fractions with denominator m, for every divisor d of m, the denominator d appears exactly $\phi(d)$ times.

It follows immediately that $\sum_{d|m} \phi(d) = m$.

Proof

- After simplification, the fraction k/d only appears if $\gcd(k, d) = 1$: for every d there are at most $\phi(d)$ such k.
- But each such k appears in the fraction kh/n, where $h \cdot d = n$.

As $g(m) = m$ is clearly multiplicative, so is ϕ!

Euler's theorem

Statement

If m and n are positive integers and $n \perp m$, then $n^{\phi(m)} \equiv 1 \pmod{m}$.

Note: Fermat's little theorem is a special case of Euler's theorem for $m = p$ prime.

Euler's theorem

Statement

If m and n are positive integers and $n \perp m$, then $n^{\phi(m)} \equiv 1 \pmod{m}$.

Note: Fermat's little theorem is a special case of Euler's theorem for $m = p$ prime.

Proof with $m \geqslant 2$ (cf. Exercise 4.32)

Let $U_m = \{0 \leqslant a < m \mid a \perp m\} = \{a_1, \ldots, a_{\phi(m)}\}$ in increasing order.

- The function $f(a) = na \pmod{m}$ is a permutation of U_m:
  If $f(a_i) = f(a_j)$, then $m \backslash n(a_i - a_j)$, which is only possible if $a_i = a_j$.
- Consequently,

$$n^{\phi(m)} \prod_{i=1}^{\phi(m)} a_i \equiv \prod_{i=1}^{\phi(m)} a_i \pmod{m}$$

- But by construction, $\prod_{i=1}^{\phi(m)} a_i \perp m$: we can thus simplify and obtain the thesis.

Warmup: $(3^{77} - 1)/2$ is odd and composite

Problem (Exercise 4.9)

Prove that $\dfrac{3^{77} - 1}{2}$ is odd and composite. *Hint:* What is $3^{77} \bmod 4$?

Warmup: $(3^{77}-1)/2$ is odd and composite

Problem (Exercise 4.9)

Prove that $\dfrac{3^{77}-1}{2}$ is odd and composite. *Hint:* What is $3^{77} \bmod 4$?

Solution

We follow the hint.

- $\phi(4) = 2$, so by Euler's theorem:

$$3^{77} = 3^{76} \cdot 3 \equiv 1 \cdot 3 = 3 \pmod 4$$

- Then $3^{77} - 1 \equiv 3 - 1 = 2 \pmod 4$, so $3^{77} - 1$ is even but not divisible by 4.
- As $3^7 - 1 \setminus 3^{77} - 1$ and $3^7 \equiv 3 \pmod 4$, $\dfrac{3^7-1}{2}$ is a factor of $\dfrac{3^{77}-1}{2}$

The Möbius function μ

Möbius function

The Möbius function μ is defined for $m \geqslant 1$ by the formula:

$$\sum_{d \mid m} \mu(d) = [m = 1]$$

m	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(m)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1

The Möbius function μ

Möbius function

The Möbius function μ is defined for $m \geqslant 1$ by the formula:

$$\sum_{d \mid m} \mu(d) = [m = 1]$$

m	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(m)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1

As $[m = 1]$ is clearly multiplicative, so is μ!

Computing the Möbius function

Theorem

For every $m \geqslant 1$,

$$\mu(m) = \begin{cases} (-1)^k & \text{if } m = p_1 p_2 \cdots p_k \text{ distinct primes}, \\ 0 & \text{if } p^2 \setminus m \text{ for some prime } p. \end{cases}$$

Indeed, let p be prime. Then, as $\mu(1) = 1$:

- $\mu(1) + \mu(p) = 0$, hence $\mu(p) = -1$.
  The first formula then follows by multiplicativity.
- $\mu(1) + \mu(p) + \mu(p^2) = 0$, hence $\mu(p^2) = 0$.
  The second formula then follows, again by multiplicativity.

Möbius inversion formula

Theorem

Let $f, g : \mathbb{Z}^+ \to \mathbb{Z}^+$. The following are equivalent:

1. For every $m \geqslant 1$, $g(m) = \sum_{d \backslash m} f(d)$.
2. For every $m \geqslant 1$, $f(m) = \sum_{d \backslash m} \mu(d) g\left(\frac{m}{d}\right)$.

Corollary

For every $m \geqslant 1$,

$$\phi(m) = \sum_{d \backslash m} \mu(d) \cdot \frac{m}{d} :$$

because we know that $\sum_{d \backslash m} \phi(d) = m$.

Proof of Möbius inversion formula

Suppose $g(m) = \sum_{d \backslash m} f(d)$ for every $m \geqslant 1$. Then for every $m \geqslant 1$:

$$\begin{aligned}
\sum_{d \backslash m} \mu(d) g\left(\frac{m}{d}\right) &= \sum_{d \backslash m} \mu\left(\frac{m}{d}\right) g(d) \\
&= \sum_{d \backslash m} \mu\left(\frac{m}{d}\right) \sum_{k \backslash d} f(k) \\
&= \sum_{k \backslash m} \left(\sum_{d \backslash (m/k)} \mu\left(\frac{m}{kd}\right) \right) f(k) \\
&= \sum_{k \backslash m} \left(\sum_{d \backslash (m/k)} \mu(d) \right) f(k) \\
&= \sum_{k \backslash m} \left[\frac{m}{k} = 1 \right] f(k) \\
&= f(m).
\end{aligned}$$

The converse implication is proved similarly.