Topic: Number Theory
Lec-2
Course: Discrete Mathematics

Divisibility

When dividing an integer by a second nonzero integer, the quotient may or may not be an integer.
For example, $12/3 = 4$ while $9/4 = 2.25$.

Definition

If a and b are integers with $a \neq 0$, we say that a *divides* b if there exists an integer c such that $b = ac$. When a divides b we say that a is a *factor* of b and that b is a *multiple* of a.
The notation $a \mid b$ denotes a divides b and $a \nmid b$ denotes a does not divide b.

The division algorithm

Let a be an integer and d a positive integer. Then, there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

- d is called the *divisor*;
- a is called the *dividend*;
- q is called the *quotient*; this can be expressed $q = a \textbf{ div } d$;
- r is called the *remainder*; this cane be expressed $r = a \textbf{ mod } d$;

Greatest Common Divisors

Definition. The *greatest common divisor* of two integers a and b, that are not both zero, is the largest integer which divides both a and b.

The greatest common divisor of a and b is written as (a, b).

Example. The common divisors of 24 and 84 are ± 1, ± 2, ± 3, ± 4, ± 6, and ± 12. Hence $(24, 84) = 12$. Similarly, looking at sets of common divisors, we find that $(15, 81) = 3, (100, 5) = 5$, $(17, 25) = 1, (0, 44) = 44, (-6, -15) = 3$, and $(-17, 289) = 17$.

We are particularly interested in pairs of integers sharing no common divisors greater than 1. Such pairs of integers are called *relatively prime*.

Definition. The integers a and b are called *relatively prime* if a and b have greatest common divisor $(a, b) = 1$.

Example. Since $(25, 42) = 1$, 25 and 42 are relatively prime.

The Euclidean Algorithm. Let $r_0 = a$ and $r_1 = b$ be nonnegative integers with $b \neq 0$. If the division algorithm is successively applied to obtain $r_j = r_{j+1}q_{j+1} + r_{j+2}$ with $0 < r_{j+2} < r_{j+1}$ for $j = 0,1,2,\ldots,n-2$ and $r_n = 0$,

$a = bq_1 + r_2 \quad 0 < r_2 < b$

then $(a, b) = r_{n-1}$, the last nonzero remainder.

Example. To find $(252, 198)$, we use the division algorithm successively to obtain

$$
\begin{aligned}
252 &= 1\cdot 198 + 54 \\
198 &= 3\cdot 54 + 36 \\
54 &= 1\cdot 36 + 18 \\
36 &= 2\cdot 18.
\end{aligned}
$$

Hence $(252, 198) = 18$.

Modular Arithmetic

Definition

If a and b are integers and m is a positive integer, then a is *congruent to* b *modulo* m if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ if this is the case, and $a \not\equiv b \pmod{m}$, otherwise.

Example. We have $22 \equiv 4 \pmod{9}$, since $9 \mid (22-4) = 18$. Likewise $3 \equiv -6 \pmod{9}$ and $200 \equiv 2 \pmod{9}$.

Theorem 3.1. If a, b, c, and m are integers with $m > 0$ such that $a \equiv b \pmod{m}$, then

(i) $a + c \equiv b + c \pmod{m}$,

(ii) $a - c \equiv b - c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

Theorem 3.2. If a, b, c and m are integers such that $m > 0$, $d = (c, m)$, and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m/d}$.

Corollary 3.1. If a, b, c, and m are integers such that $m > 0$, $(c,m) = 1$, and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.

Theorem 3.3. If a, b, c, d, and m are integers such that $m > 0$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then

(i) $a + c \equiv b + d \pmod{m}$,

(ii) $a - c \equiv b - d \pmod{m}$,

(iii) $ac \equiv bd \pmod{m}$.

Theorem 3.5. If a, b, k, and m are integers such that $k > 0$, $m > 0$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.

Theorem 3.6. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots,$ $a \equiv b \pmod{m_k}$ where $a, b, m_1, m_2, \ldots, m_k$ are integers with $m_1, m_2, \ldots, m_k$ positive, then

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]},$$

where $[m_1, m_2, \ldots, m_k]$ is the least common multiple of $m_1, m_2, \ldots, m_k$.

Corollary 3.2. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots,$ $a \equiv b \pmod{m_k}$ where a and b are integers and $m_1, m_2, \ldots, m_k$ are relatively prime positive integers, then

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

Theorem 20.1.7: **A linear congruence $ax \equiv b \bmod m$ has solutions if and only if $gcd(a, m) \mid b$.**
(in which case it has precisely $gcd(a, m)$ different solutions modulo m)

How can we solve it, i.e. find all integers x that satisfy it?

One possible method is to multiply both sides of the congruence by an inverse $\overline{a}$ of $a \pmod{m}$ if one such inverse exists:
$\overline{a}$ is an **inverse** of $a \pmod{m}$ if $\overline{a}a \equiv 1 \pmod{m}$.

Fermat's Little Theorem

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

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

Furthermore, for every integer a we have

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

Example: $p = 5$

Verify that the theorem works for $a = 1, 2, 3, 4$: For 1 it is trivial,
$2^4 = 16 \equiv 1 \pmod{5}$, $3^4 = 81 \equiv 1 \pmod{5}$, $4^4 = 256 \equiv 1 \pmod{5}$.

Find 7^{222} **mod** 11.

Solution: We can use Fermat's little theorem to evaluate 7^{222} **mod** 11 rather than using the fast modular exponentiation algorithm. By Fermat's little theorem we know that $7^{10} \equiv 1 \pmod{11}$, so $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer k. To take advantage of this last congruence, we divide the exponent 222 by 10, finding that $222 = 22 \cdot 10 + 2$. We now see that

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

It follows that 7^{222} **mod** $11 = 5$. ◀

Show that

$$3^{302} \equiv 4 \mod 5.$$

Solution: From Fermat's theorem

$$3^4 \equiv 1 \mod 5$$

$$\Rightarrow (3^4)^{75} \equiv 1^{75} \mod 5$$

$$\Rightarrow 3^{300} \equiv 1 \mod 5$$

$$\Rightarrow 3^{300} \cdot 3^2 \equiv 3^2 \mod 5$$

$$\Rightarrow 3^{302} \equiv 9 \mod 5 \equiv 4 \mod 5$$

Show that

$$17 | 2^{3n+1} + 3.5^{2n+1}.$$

Solution: We need to prove that $2^{3n+1} \equiv -3.5^{2n+1} \mod 17$.

$$8 \equiv 25 \mod 17$$

$$\Rightarrow 8^n \equiv 25^n \mod 17$$

$$\Rightarrow 2^{3n} \equiv 5^{2n} \mod 17$$

Also

$$2 \equiv -15 \mod 17 \qquad \Rightarrow 2^{3n} \cdot 2 \equiv -15 \cdot 5^{2n} \mod 17$$

$$\Rightarrow 2^{3n+1} \equiv -3.5^{2n+1} \mod 17.$$

Problem

Show that $2^{41} \equiv 3 \mod 23$.

Solution:

$2^{22} \equiv 1 \mod 23$ From Fermat's theorem

$$\Rightarrow 2^{44} \equiv 1 \mod 23$$

$$\Rightarrow 2^{44} \equiv 24 \mod 23$$

$$\Rightarrow 2^{41} \cdot 8 \equiv 3 \cdot 8 \mod 23$$

$$\Rightarrow 2^{41} \equiv 3 \mod 23 \qquad \text{as } \gcd(8, 23) = 1.$$

Prove that for all integers $n \geq 1$

1. $3^{3n+1} \equiv 3 \cdot 4^{2n} \mod 11$
2. $11 | 3^{3n+2} + 2 \cdot 5^n$

RSA public key cryptosystem

RSA is based on modular arithmetic and large primes, and its security comes from the computational difficulty of factoring large numbers.

The *key generation* works as follows:

select p and q to be large primes (at least several hundreds of digits); the degree of security is dependent on the size of p and q. Take $n = pq$.

Then the **public key** is a pair $k = (n, e)$ such that

$$gcd(e, (p-1)(q-1)) = 1.$$

The **enconding function** is

$$f(m, k) = m^e \bmod n.$$

This assumes that the message can be represented by an integer $m < n$ with gcd$(m, p) = 1 =$gcd(m, q); if not we can break m down into smaller pieces and encode each individually.

The **private key** is a pair $k' = (n, d)$ such that

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

The decoding function is

$$g(c, k') = c^d \bmod n.$$

The security of the algorithm lies in the challenge of *prime factorization*: in order to calculate d it is necessary tp factor n to get p and q, which is very difficult (we only know methods that are exponential on the number of digits in p and q).
We now show that RSA actually works.

Example:

Bob generates his pair of private/secret keys. He selects two primes $p = 43$ and $q = 59$ (this primes are small in our example but should be huge for RSA be difficult to be broken).
Then $n = pq = 2537$.
Since Bob has p and q he calculates $(p-1)(q-1) = 2436$
He chooses $e = 13$, which is valid since
gcd$(e, (p-1)(q-1))$ =gcd$(13, 2436) = 1$.
Bob calculates the inverse of $13 \pmod{(p-1)(q-1) = 2436}$, which is $d = 937$.
(You can check that
$de \equiv 937 \times 13 \equiv 12181 \equiv 5 \times 2436 + 1 \equiv 1 \pmod{2436}$.
Thus, Bob private key is $(2436, 937)$, which he keeps screte, and Bob's public key is $(2436, 13)$, which he publishes in his web site.

(example continued)

Alice wants to send the message "STOP" to Bob using RSA. She encodes this:

S→ 18, T→ 19, O→ 14, P→ 15, and sends the message: 1819 1415 (group in blocks of 4 digits).

This $m = m_1||m_2$. Each block m_i is encrypted:

$$\begin{aligned} 1819^{13} \mod 2537 &= 2081 \\ 1415^{13} \mod 2537 &= 2182 \end{aligned}$$

Biob receives 2081 2182 and he decodes each number (block), using his private key:

$$\begin{aligned} 2081^{937} \mod 2537 &= 2081 \to ST \\ 2182^{937} \mod 2537 &= 1415 \to OP \end{aligned}$$

1819

Thus the message sent by Alice was STOP.

To be continued……

Thanks for watching

Have a nice day