CONGRUENCES

Modular arithmetic. Two whole numbers a and b are said to be *congruent modulo* n if they give the same remainders when divided by n. In other words, the difference $a - b$ is divisible by n.

Examples: $5 \equiv 1 \pmod 2$, $6 \equiv 2 \pmod 4$, etc.

Congruences are very important because many of their properties are similar to properties of ordinary equality.

Properties of Congruences:

(1) $a \equiv a \pmod d$
(2) $a \equiv b \pmod d$ implies $b \equiv a \pmod d$
(3) If $a \equiv b \pmod d$ and $b \equiv c \pmod d$, then $a \equiv c \pmod d$.
(4) If $a \equiv a' \pmod d$ and $b \equiv b' \pmod d$, then
   - $a \pm b \equiv a' \pm b' \pmod d$
   - $ab \equiv a'b' \pmod d$.

Geometric representation: To represent numbers modulo d use a circle divided into d equal parts. Any integer divided by d gives one of the remainders $0, 1, \ldots, d-1$. Place these numbers at equal intervals on the circumference of the circle. Every integer is congruent modulo d to one of those numbers and is geometrically represented by one of those points. If you look at a regular clock, you will see exactly such a picture, with $d = 12$.

Modular arithmetics with $d = p$ being a prime number are particularly important. Let $\mathbb{Z}_p$ denote the set of remainders with respect to a prime p. Operations (addition and multiplication) on this set are induced by the odinary addition and multiplication on integers.

Problem 1. Construct the multiplication tables in the cases of $p = 4$ and $p = 5$.

Problem 2. Use modular arithmetic to solve the following:

(1) A biology experiment starts at 2 p.m. and lasts 80 hours. At what time of the day will the experiment end?
(2) What day of the week will your birthday be in 2011? (There are no leap years between now and 2011).

Problem 3. Let

$$z = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n$$

be a number. Then $a_n, a_{n-1}, \ldots, a_0$ are the digits used in the decimal notation for z. Prove the following divisibility tests:

(1) Show that a number is divisible by 3 if and only if the sum of its digits is divisible by 3.
(2) Show that a number is divisible by 11 if and only if the *alternating* sum of its digits is divisible by 11.

(3) Show that a number is divisible by 7 if and only if the expression

$$r = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + \dots$$

is divisible by 7.

(*Hint:* First, determine the remainders of powers of 10 with respect to 3, 11 and 7 respectively).

Problem 4. Use properties of congruences:

(1) To what number between 0 and 6 inclusive is the product $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$ congruent modulo 7?
(2) To what number between 0 and 12 inclusive is the product

$$3 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 29 \cdot 113$$

congruent modulo 13?

Euclid's Lemma.

Lemma. *(A characterization of prime numbers)*
A number p is prime if and only if the following is true:
p divides $a \cdot b$ implies that either p divides a or p divides b.

Proof. Proof both directions as an exercise. □

In other words, the Lemma says that there is no divisors of 0 in modular arithmetic modulo a prime number.

Problem 5. (Division in modular arithmetic) Show that division works properly, i.e. the cancellation law

$$a \cdot k \equiv b \cdot k \pmod{d} \implies a \equiv b \pmod{d}$$

holds, if and only if the module d is prime. (If $d = p$ is prime, show that Euclid's lemma guarantees that the division works properly. If the module, d, is not prime, show by example how the division fails its properties).

Euclidean Algorithm. To find the gratest common divisor, $\gcd(a, b)$, of two numbers, a and b, one uses the Euclidean Algorithm.

Main idea: If $a = b \cdot q + r$ for some integers $a,\ b,\ q$ and r , then $\gcd(a, b) = \gcd(b, r)$.

Euclidean algorithm: To find $\gcd(a, b)$, use successive division as follows:

$$\begin{aligned} a &= bq_1 + r_1 && (0 < r_1 < b) \\ b &= r_1q_2 + r_2 && (0 < r_2 < r_1) \\ r_1 &= r_2q_3 + r_3 && (0 < r_3 < r_2) \\ r_2 &= r_3q_4 + r_4 && (0 < r_4 < r_3) \\ \dots &\ \dots\ \dots \end{aligned}$$

continuing as long as the remainder is above 0. We are, therefore, constructing a decreasing sequence of remainders:

$$b > r_1 > r_2 > r_3 > \cdots > 0$$

Hence after a finite number of steps, we will get remainder equal to 0, i.e, $r_{n-1} = r_nq_{n+1} + 0$. When this is the case, we conclude that $\gcd(a, b) = r_n$. In other words,

the greatest common divisor of a and b is the last positive remainder in the sequence of remainders obtained by the Euclidean algorithm.

Problem 6. Carry out the Euclidean algorithm for the pair $a = 245$, $b = 193$.

Theorem 7. *(Bezout) If $d = gcd(a, b)$, then there are exist integers k and l such that $d = ka + lb$. In particular, for any pair of numbers a and b which are relatively prime, one can write $1 = ka + lb$ for some integers k and l.*

Proof. Exercise. □

Fermat's Theorem.

Theorem. *(Fermat, 1640) Let p be a prime number which does not divide a. Then*

$$a^{p-1} \equiv 1 \ (mod\ p)$$

In other words, $a^{p-1} - 1$ is divisible by p.

Proof. We will go through the proof by in two steps:

Step 1: Consider the first $(p-1)$ multiples of a:

$$a, \quad 2a, \quad 3a, \quad \ldots, (p-1)a. \tag{0.1}$$

First we will show that when we take these numbers modulo p, we just get a rearrangement of the set of $p-1$ remainders modulo p.

$$1,\ 2,\ 3,\ \ldots, (p-1).$$

Argue by contradiction: assume that we do not get some of the remainders. Then, the remainders for at least two of the numbers in (0.1) are the same. I.e.,

$$ka \equiv la \ (\text{mod } p)$$

for some $1 \leq k < l \leq p-1$. This means that $(k-l)a \equiv 0 \ (\text{mod } p)$. Prove that this is impossible: Conclude that

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \ \equiv (p-1)! \ (\text{mod } p)$$

Step 2. Using the last congruence relation, conclude the statement of FLT. □

Problem 8. Show that

(1) $2^8 \equiv 1$ (mod17).
(2) $3^8 \equiv -1$ (mod17).
(3) $3^{14} \equiv -1$ (mod29).
(4) $2^{14} \equiv -1$ (mod 29).

Wilson's theorem.

Theorem. *(Wilson) A number p is prime if and only if*

$$(p-1)! \equiv -1 \ (modp)$$

In other word, if and only if $(p-1)!+1$ is divisible by p.

Proof. For $p = 2$ and $p = 3$ it is easy to check the statement directly:

" $\Longrightarrow$ ": Assume that $p > 3$ is prime. Then each of the numbers $2, 3, \ldots, p-1$ is relatively prime with p. Therefore, for any $k \in \{2, 3, \ldots, p-1\}$ there is a unique $l \in \{2, 3, \ldots, p-1\}$ such that

$$k \cdot l \equiv 1 \ (\text{mod } p)$$

Moreover, $l = k$ if and only if $k = 1$ or $p-1$. Therefore, we can divide the set of numbers $\{2, 3, \ldots, p-2\}$ into pair (k, l) such that $k \cdot l \equiv 1 \ (\text{mod}p)$ for every pair. Hence,

$$2 \cdot 3 \cdot \cdots \cdot (p-3) \cdot (p-2) \equiv 1 \ (\text{mod}p).$$

Multiplyinig by $p - 1 \equiv -1 \ (\text{mod}p)$ we get the statement of Wilson's theorem.

" $\Longleftarrow$ " If p is not prime, then some of the numbers in the set $(2, 3 \ldots, p-1\}$ are not relatively prime with p. Therefore, $\gcd((p-1)!,\ p) > 1$, which contradicts $(p-1)! \equiv -1 \ (\text{mod}p)$. □

Problem 9. Let $p = 13$. Pair up the numbers in the set $\{2, 3, \ldots, 12\}$ so that for every pair (k, l) we have $k \cdot l \equiv 1 \ (\text{mod}13)$. Then check the statement of Wilson's theorem for $p = 13$.

Problem 10. Can you say more about $(n-1)!$ modulo n when n is composite?

Problem 11. Use Wilson's theorem to

(1) compute 14! modulo 17.
(2) compute 19! modulo 17.