Number Theory Section Summary: 4.1-2

The Theory of Congruences

1. Summary

Carl (or Karl) Friedrich Gauss, prince of mathematicians, thought that "Mathematics is the queen of the sciences and number-theory the queen of mathematics." His *Disquisitiones Arithmeticae* was the book Dirichlet carried about like the Bible. This notion of **congruence** appears in the first chapter....

You're probably already familiar with modular arithmetic: this is the generalization of it. On the clock, 13 and 1 are the same thing (if we ignore pm and am – 25 and 1 work if you don't want to ignore am and pm!).

2. Definitions

Definition 4.1: Let n be a fixed positive integer. Two integers a and b are said to be **congruent modulo** n, symbolized by

$$a \equiv b (\text{mod } n)$$

if n divides $a - b$; that is, provided $a - b = kn$ for some integer k.

complete set of residues: a collection of n integers $a_1, a_2, \ldots, a_n$ forms a **complete set of residues modulo** n if every integer is congruent modulo n to one and only one of the collection. (For those of you who've had linear algebra, you can think of the collection as a "basis" for all integers with respect to the operation of congruence).

3. Theorems

Theorem 4.1: For arbitrary integers a and b, $a \equiv b(\text{mod } n)$ if and only if a and b leave the same nonnegative remainder when divided by n.

$$\left.\begin{array}{l} a = q_1 n + r \\ b = q_2 n + r \end{array}\right\} \Rightarrow a - b = (q_1 - q_2) n \Leftrightarrow a \equiv b \ (\text{mod } n)$$

Theorem 4.2: Let $n > 1$ be fixed and a, b, c, and d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a (\text{mod } n)$

(b) If $a \equiv b (\text{mod } n)$, then $b \equiv a (\text{mod } n)$.

(c) If $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$, then $a \equiv c (\text{mod } n)$.

(d) If $a \equiv b (\text{mod } n)$ and $c \equiv d (\text{mod } n)$, then $a + c \equiv b + d (\text{mod } n)$, and $ac \equiv bd (\text{mod } n)$.

(e) If $a \equiv b (\text{mod } n)$, then $a + c \equiv b + c (\text{mod } n)$, and $ac \equiv bc (\text{mod } n)$.

(f) If $a \equiv b (\text{mod } n)$, then $a^k \equiv b^k (\text{mod } n)$ for any positive integer k.

Note that the converse of Theorem 4.2(f) is false: for example

$$2^2 \equiv 4^2 (\text{mod } 4) \quad \text{but} \quad 2 \not\equiv 4 (\text{mod } 4)$$

Half of the converse of Theorem 4.2(e) is also false, as indicated in Theorem 4.3:

Theorem 4.3: If $ca \equiv cb (\text{mod } n)$, then $a \equiv b (\text{mod } n/d)$, where $d = \gcd(c, n)$.

$6 \equiv 3 \text{ mod } 3$

$4 \cdot 6 \equiv 4 \cdot 3 \ (\text{mod } 12) \quad \not\Rightarrow \quad 6 \equiv 3 \ (\text{mod } 12)$!

[Unless 6 o'clock is the same as 3 o'clock!]

Good things happen when $\gcd(c, n) = 1$: we can cancel c's with joyful abandon!

Corollary 1: If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Corollary 2: If $ca \equiv cb \pmod{p}$ (p prime), and p does not divide c, then $a \equiv b \pmod{p}$.

Unfortunately we cannot simply cancel without thought: for example, you can check that

$$2 \cdot 6 \equiv 2 \cdot 12 \pmod{12}$$

but that

$$6 \not\equiv 12 \pmod{12}$$

In fact, however, it is true that

$$6 \equiv 12 \pmod{6}$$

4. Properties/Tricks/Hints/Etc.

Because all integers are congruent modulo 1, we generally assume that in a formula mod n, $n > 1$.

Note that $ab \equiv 0 \pmod{n}$ does not imply that a or b is 0 (mod n): for example $3 \cdot 5 \equiv 0 \pmod{15}$ but neither 5 nor 3 is 0 (mod 15). What we can say is that, if $ab \equiv 0 \pmod{n}$ and $\gcd(a, n) = 1$, then $b \equiv 0 \pmod{n}$.