Number Theory Section Summary: 4.1-2
The Theory of Congruences

1. Summary

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 module 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 module n** if every integer is congruent module 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.

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

(a) $a \equiv a \pmod{n}$

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

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

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

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

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

$n \mid a-b$ or $a = kn + b$, so $a^k = (kn+b)^k$ expand using Binomial Theorem

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

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

$a^k = kn + b^k$

$n \mid a^k - b^k$

4. Properties/Tricks/Hints/Etc.

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

#66) $13 \mid 3^{n+2} + 4^{2n+1}$

$\equiv 0 \pmod{13}$

Consider $3^{n+2} + 4^{2n+1}$

$= 3^2 \cdot 3^n + 4 \cdot (4^2)^n$

$16 = 13 + 3$

$16^n = (13+3)^n$

$= 9 \cdot 3^n + 4 \cdot (16)^n$

$\equiv 9 \cdot 3^n + 4 \cdot (3)^n \pmod{13}$

$\equiv 13 \cdot 3^n \pmod{13}$

$\equiv 0 \pmod{13}$

#6c $27 \mid 2^{5n+1} + 5^{n+2}$

$2^{5n+1} + 5^{n+2}$

$= 2 \cdot (2^5)^n + 5^2 \cdot 5^n$

$\equiv 2 \cdot (5)^n + 25 \cdot 5^n \pmod{27}$

$\equiv 27 \cdot 5^n \pmod{27}$

$\equiv 0 \pmod{27}$

#8b $a \in \mathbb{Z} \Rightarrow a^3 \equiv 0, 1 \text{ or } 6 \pmod 7$

$a = 7n + i$, $i = 0, 1, \ldots, 6$

$a \equiv i \pmod 7$ so $a^3 \equiv i^3 \pmod 7$

i	0	1	2	3	4	5	6
$i^3 \pmod 7$	0	1	1	6	1	6	6

Consider the converse of (e) Theorem 4.2

Is it true that

If $ca \equiv cb \pmod n$ then

$a \equiv b \pmod n$?

Is cancellation always permitted?

$\begin{cases} ca = cb + nk \\ c(a-b) = nk \end{cases}$

$2 \cdot 5 \equiv 2 \cdot 4 \pmod 2$, but

$5 \not\equiv 4 \pmod 2$

No!

Consider the converse to (f): is it true that

if $a^k \equiv b^k \pmod n$ then

$a \equiv b \pmod n$?

$a = 2$
$b = 3$
$n = 5$
$k = 2$

$2^2 \equiv 3^2 \pmod 5$ ✓

but $2 \not\equiv 3 \pmod 5$

If $a \cdot b \equiv 0 \pmod n$, what can you conclude about a and/or b?

$a \cdot b = nk$ for some $k \in \mathbb{Z}$.

$\therefore$ n divides the product $a \cdot b$.

If n is prime, then $n \mid a$ or $n \mid b$;
WLOG assume $n \mid a \iff a \equiv 0 \pmod n$
If $\gcd(n, a) = 1$ (again, WLOG), then
$n \mid b$ and $b \equiv 0 \pmod n$.

Watch out for this:

$3 \cdot 5 \equiv 0 \pmod{15}$,
but neither 3 nor $5 \equiv 0 \pmod{15}$.

4b p 67 What is the remainder when $S = \sum_{i=1}^{100} i^5$ is divided by 4?

Q: What is $S \pmod 4$?

Observation: every integer is $0, 1, 2, 3 \pmod 4$.

$0 \pmod 4$ $\quad$ $0 \pmod 4$ $\quad$ $0 \pmod 4$

$$S = 1^5 + 2^5 + 3^5 + 4^5 + 5^5 + \ldots + 9^5 + \ldots + 100^5$$

$$\equiv \sum_{i=1}^{25} (0)^5 + \sum_{i=1}^{25} (1)^5 + \sum_{i=1}^{25} (2)^5 + \sum_{i=1}^{25} (3)^5 \pmod 4$$

$$\equiv 25 + 25(3^5) \pmod 4$$

$$\equiv 25 + 25(-1)^5 \pmod 4$$

$$\equiv 0 \pmod 4$$