LAST HANDOUT: Prime numbers and some related facts (Ch 23-24)

Definition: An integer $n \geq 2$ is said to be **prime** if and only if the only positive divisors of *n* are 1 and *n*
(and it's called **composite** otherwise).

Some examples: primes: 2, 3, 5, 7, … *Not primes: -1, 1, 0, 6, 21, 51*

Thm 23.1.3 (and its converse) (Euclid): **An integer $p \geq 2$ is a prime number if and only if $\forall\, a, b \in \mathbb{Z}$,**

$$p|ab \Rightarrow (p|a \text{ or } p|b)\,.$$

Example: 5|ab ⇔ 5|a or 5|b, but a composite number like 10 can divide ab=(4)(15)=60 without dividing either factor.

Thm 23.3.1 (Fundamental Theorem of Arithmetic) (19th century)

Every positive integer $n \geq 2$ can be written uniquely as a product of powers of prime factors (wih the prime factors in the product written in increasing order):

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

where $p_1 < p_2 < \cdots < p_k$ are prime numbers, $k \geq 1$, and the exponents $\alpha_i \in \mathbb{Z}^+$.

(Proof: existence: by induction prop 23.1.2 pg 278, uniqueness: by contradiction on pg 283)

Examples: $200 = 2^3 \times 5^2, 81 = 3^4$*, etc*

Note: One can use the prime factorization of an integer n, if known, to determine all the divisors of n.
Also, if we know the prime factorization of two integers a and b, we can determine the greatest common divisor. How?

Ex: 180=??

126=??

Gcd(126, 180)=??

Thm 23.5.1: **There are infinitely many prime numbers** (one of the "Proofs from the Book")

Proof:
Suppose, by contradiction, that there are only finitely many prime numbers: $p_1, p_2, p_3, \ldots p_k$ for some $k \in \mathbb{Z}^+$.
Consider the integer $n = p_1 p_2 p_3 \ldots p_k + 1$. This integer is not divisible by any of the prime numbers p_i because

$$n \equiv \_\_\_\_\_ \mod p_i$$

This means that n cannot be written as a product of prime factors, which contradicts FTA. QED

Searching for large prime numbers is a favorite past time of many mathematicians who have access to powerful computers. Currently, the largest known prime is: $2^{43112609}-1$ *(about 12.9 million digits, Aug 08).*

(Curious for more? See http://primes.utm.edu/largest.html)

A few fun results about congruences modulo prime numbers, courtesy of 17th & 18th century mathematicians:

Fermat's Little Theorem: (stated by Fermat, proved by Euler & others)

If ***p* is a prime number** and ***a* is a positive integer not divisible by *p***, then $a^{p-1} \equiv 1\ mod\ p$.

(Cute proof on page 290, if curious)

Example: $6^{12} \equiv 1 \bmod 13$.

More interesting application: What is the reminder of 3^{304} modulo 11?

p=11 is a prime, and 11 does not divide a=3. Hence, by FLT: ???_____

So, $3^{304} = 3^{300}3^4 = (\quad)^{30}3^4 \equiv (\quad)(\,81\,) \bmod 11 \equiv 11 * 7 + 4 \bmod 11 \equiv 4 \bmod 11.$

Wilson's Theorem: (conjectured by Wilson, proved by Lagrange)

If p is a prime number, then $(p-1)! \equiv -1 \bmod p$

(converse is also true) (proof in book and in solved pbls)

Example: $10! \equiv -1 \bmod 11$

Example: What is the remainder for $16!$ divided by 19?

Since 19 is a prime, by Wilson's Theorem, $18! \equiv -1 \bmod 19$.

But, $18! = 16!\,(17)(18)$, so:

$$16!\,(17)(18) \equiv -1 \bmod 19$$

$$16!\,(-2)(-1) \equiv -1 \bmod 19$$

$$16!\,(2) \equiv 18 \bmod 19$$

By prop 19.3.2 (since 2 does not divide 19):

$$16! \equiv 9 \bmod 19$$

For Hwk 8, Pbl 7 (iii): note that 437 is NOT a prime, but can be written as the product of two primes.

THE END