University of Waterloo
Faculty of Mathematics

Centre for Education in
Mathematics and Computing

Senior Math Circles
October 15, 2008
Number Theory II

Number Theory

More Divisibility:

Example: Prove that, for integers n with $n > 2$, if one of $2^n + 1$ or $2^n - 1$ is prime, then the other is composite.
Solution:
The numbers $2^n - 1, 2^n$, and $2^n + 1$ are three consecutive integers, and therefore one of them must be divisible by 3. Since 2^n is a power of 2, it will not have any factors of 3. Therefore, either $2^n - 1$ or $2^n + 1$ is divisible by 3. If one is prime, it cannot be divisible by 3, so the other one must be, and is therefore composite.

Euler ϕ Function:

Example: Find $\phi(96059601)$.
Solution:
To find $\phi(96059601)$, first factor 96059601.
$96059601 = 3^8 \cdot 11^4$

$$\begin{aligned} \text{Therefore } \phi(96059601) &= 96059601 - \tfrac{96059601}{3} - \tfrac{96059601}{11} + \tfrac{96059601}{33} \\ &= 96059601 - 32019867 - 8732691 + 2910897 \\ &= 58217940 \end{aligned}$$

Formulae:
If p is a prime number, then $\phi(p) = p - 1$ and $\phi(p^a) = p^a - p^{a-1}$.
If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Congruences:

Defintion:
If $n|a-b$ then we write $a \equiv b \mod n$. This means that when n is divided into a and n is divided into b, the remainder will be the same.

$13 \equiv 19 \mod 6$
$14 \equiv 2 \mod 12$
$10 \equiv -5 \mod 3$

When solving for x in congruences, we write it in the simplest form, $x \equiv a \mod n$ where $0 \leq a < n$.

Problems:
Find x

1. $x \equiv 19 \mod 5$
2. $x \equiv 96059601 \mod 10$

Properties of congruences:

1. $a \equiv a \mod n$
2. If $a \equiv b \mod n$ and $b \equiv c \mod n$ then $a \equiv c \mod n$.
3. $a \equiv b \mod n$ implies $b \equiv a \mod n$
4. If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.

Example: $2x \equiv 7 \mod 9$
Solution:
$2x \equiv 7 \mod 9$
$10x \equiv 35 \mod 9$
$x \equiv 8 \mod 9$

Problems:
Solve for x.

1. $3x \equiv -2 \mod 5$
2. $4x \equiv 19 \mod 7$

More Properties:
a) If $\gcd(a, n) = 1$ and $ab \equiv ac \mod n$ then $b \equiv c \mod n$.
b) If $\gcd(a, n) = d$ and $ab \equiv ac \mod n$ then $b \equiv c \mod \frac{n}{d}$.

Example: $6x \equiv 12 \mod 10$
Solution:
$\gcd(6, 10) = 2$
and $6x \equiv 6(2) \mod 10$
so $x \equiv 2 \mod 5$
Therefore, $x \equiv 2 \mod 10$ or $x \equiv 7 \mod 10$.

Problem:
$3x \equiv 6 \mod 9$

Fermat-Euler Theorem:

If $\gcd(a, N) = 1$, then $a^{\phi(N)} \equiv 1 \mod N$.
Corollary: Fermat's Little Theorem
If p is prime, then $a^{p-1} \equiv 1 \mod p$.

Example: Find the last two digits of 3^{3141}.
Solution:
To find the last two digits of 3^{3141}, we want to figure out what the number is congruent to modulo 100.

By the Fermat-Euler Theorem, we know $3^{\phi(100)} \equiv 1 \mod 100$,
since $\gcd(3, 100) = 1$.

$$\begin{aligned} \text{Now, } \phi(100) &= \phi(4)\phi(25) \\ &= (4-2)(25-5) \\ &= 40 \end{aligned}$$

Therefore, $3^{40} \equiv 1 \mod 100$.

$$\begin{aligned} \text{As a result, } 3^{3141} &\equiv (3^{40})^{78} \cdot 3^{21} \mod 100 \\ &\equiv (1)^{78} \cdot 3^{21} \mod 100 \\ &\equiv 3^{21} \mod 100 \end{aligned}$$

To quickly find $3^{21} \mod 100$, we will use the square and multiply algorithm.
$3^1 \equiv 3 \mod 100$
$3^2 \equiv 9 \mod 100$
$3^4 \equiv 9^2 \equiv 81 \mod 100$
$3^8 \equiv 6561 \equiv 61 \mod 100$
$3^{16} \equiv 3721 \equiv 21 \mod 100$

$$\begin{aligned} 3^{21} &\equiv 3^{16} \cdot 3^4 \cdot 3 \mod 100 \\ &\equiv (21)(81)(3) \mod 100 \\ &\equiv 5103 \mod 100 \\ &\equiv 3 \mod 100 \end{aligned}$$

Therefore, the last two digits of 3^{3141} are 03.

Divisibility Criteria:

A number is divisible by 3 if the sum of its digits is divisible by 3.

Proof:
Let $n = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$, then

$$\begin{aligned} n &\equiv a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 \mod 3 \\ &\equiv a_m (1)^m + a_{m-1}(1)^{m-1} + \cdots + a_1 (1) + a_0 \mod 3 \\ &\equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \mod 3 \end{aligned}$$

Problem Set

1. Calculate $\phi(3375)$ and $\phi(5445)$.
2. Prove that if p and $8p^2 + 1$ are prime, then $8p^2 - 1$ is also prime.
3. Find the last two digits of 2009^{2008}.
4. Let $N = 3^{105} + 4^{105}$. Prove that $7|N$ and find $N \mod 11$.
5. Without using a calculator, find the last two digits of 19^{19}.
6. Determine the criteria for an integer to be divisible by 11.
7. Prove that $p^2 \equiv 1 \mod 12$ for every prime number $p > 3$.
8. Find the last 3 digits of 7^{9999}.