Number Theory - MTSC 317
Lecture 1

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

August 29, 2014

1 Introduction

The branch of mathematics that deals with properties of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ or natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ has been traditionally called Number Theory.

Number Theory is a significant topic because:

- It is a basic piece of math as you can build other fields from natural numbers:

$$\mathbb{N} \xrightarrow{negation} \mathbb{Z} \xrightarrow{division} \mathbb{Q} \xrightarrow{\text{real analysis}} \mathbb{R} \xrightarrow{\sqrt{-1}} \mathbb{C}.$$

- It is an elegant field.

> "Mathematics is the queen of sciences and number theory is the queen of mathematics."
>
> \- Carl Friedrich Gauss

  Number theory uses techniques from algebra, analysis, geometry, logic, computer science and contributes to the development of these fields.

- Number theory finds applications in different fields such as RSA public key cryptography and coding theory.

- It's very useful for learning and utilizing rules of logic, reading and writing proofs.
- There are several basic problems formulated as conjectures that have not been solved yet.

2 Mathematical Induction

Definition 2.1 (Well-ordering Principle)**.** Every nonempty set S of nonnegative integers contains a least element. Thus, there is some integer a in S such that $a \leq b$ for all b's in S.

Theorem 2.2 (The Archimedean Property)**.** *If a and b are any positive integers, then there exists a positive integer n such that $n \cdot a \geq b$.*

Theorem 2.3 (First Principle of Finite (or Mathematical) Induction)**.** *Let S be a set of positive integers with the properties:*

1. *Integer 1 belongs to S.*
2. *Whenever integer k is in S, the next integer $k+1$ must also be in S.*

Then S is the set of all positive integers.

Example 2.1. Show that

$$1 + 2 + 2^2 + \ldots + 2^{n-1} = 2^n - 1, \forall n \in \mathbb{N}, n > 0.$$

Proof. Let S be the set of positive integers n for which our equation holds.

Basis for the induction – For $n = 1$, $2^1 - 1 = 2 - 1 = 1$, therefore our equation holds.

Induction hypothesis – We assume that $1 + 2 + 2^2 + \ldots + 2^{k-1} = 2^k - 1$ for $k \in S$.

Induction step – For $k+1$ we have that

$$
\begin{aligned}
&1 + 2 + 2^2 + \ldots + 2^{k-1+1} \\
&= 1 + 2 + 2^2 + \ldots + 2^{k-1} + 2^{k-1+1} \\
&= 2^k - 1 + 2^k \\
&= 2 \cdot 2^k - 1 \\
&= 2^{k+1} - 1.
\end{aligned}
$$

Hence, $1 + 2 + 2^2 + \ldots + 2^n - 1, \forall n \in \mathbb{N}, n > 0$ holds for $n = k + 1$ if it holds for $n = k$.

By the induction principle, S must be the set of all positive integers, i.e. $S = \mathbb{Z}$. $\square$

Theorem 2.4 (Second Principle of Finite Induction)**.** *Let S be the set of positive integers with the properties*

1. *1 belongs to S,*
2. *If k is a positive integer such that $1, 2, \ldots, k$ belong to S, then $k + 1$ must also belong to S,*

then S is the set of all positive integers, i.e. $S = \mathbb{Z}$.

Mathematical Induction is widely used for definitions or proofs.

For example $n!$ can be defined as

1. $1! = 1$
2. $n! = n \cdot (n - 1)!$ for $n > 1$.

Example 2.2. Let the sequence defined as $a_1 = 1$, $a_2 = 3$, $a_n = a_{n-1} + a_{n-2}$.

Show that $a_n < (7/4)^n$ holds for all positive integers n.

Proof. For $n = 1$, $a_1 = 1 < \frac{7}{4}$.

For $n = 2$, $a_2 = 3 < (7/4)^2 = \frac{49}{16}$.

Let $a_n < (7/4)^n$ for $n = 1, 2, \ldots, k-1$.

Then

$$\begin{aligned}
a_k &= a_{k-1} + a_{k-2} < (\frac{7}{4})^{k-1} + (\frac{7}{4})^{k-2} \\
&= a_{k-1} + a_{k-2} < (\frac{7}{4})^{k-2}(\frac{7}{4} + 1) \\
&= a_{k-1} + a_{k-2} < (\frac{7}{4})^{k-2}(11/4) < (\frac{7}{4})^{k-2}(7/4)^2 \\
&= a_{k-1} + a_{k-2} < (\frac{7}{4})^{k} \\
a_k &< (\frac{7}{4})^{k}.
\end{aligned}$$

By the second principle of finite induction it follows that $a_n < (7/4)^n$, $\forall n \in \mathbb{N}^*$. $\square$

Number Theory - MTSC 317
Lecture 2

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

August 29, 2014

1 The Binomial Theorem

Definition 1.1. The binomial coefficients $\binom{n}{k}$ for any positive integer n and any integer k with $0 \le k \le n$ are defined by

$$\binom{n}{r} = \frac{n!}{k!(n-k)}.$$

Example:

$$\binom{8}{3} = \frac{8!}{3!5!} = \frac{8 \cdot 7 \cdot 6 \cdot 5!}{3!5!} = \frac{8 \cdot 7 \cdot 6}{3 \cdot 2 \cdot 1} = 56.$$

Theorem 1.2 (Pascal's Rule)**.**

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

Proof.

$$\begin{aligned}
\frac{1}{k}+\frac{1}{n-k+1} &= \frac{n-k+1+k}{k(n-k+1)} = \frac{n+1}{k(n-k+1)} \\
\left(\frac{n!}{(k-1)!(n-k)!}\right)\left(\frac{1}{k}+\frac{1}{n-k+1}\right) &= \frac{n!(n+1)}{(k-1)!(n-k)!k(n-k+1)} \\
\frac{n!}{(k-1)!(n-k)!k}+\frac{n!}{(k-1)!(n-k)!(n-k+1)} &= \frac{n!(n+1)}{(k-1)!(n-k)!k(n-k+1)} \\
\frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)!} &= \frac{(n+1)!}{k!(n-k+1)!} \\
\frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-(k-1))!} &= \frac{(n+1)!}{k!(n+1-k)!} \\
\binom{n}{k}+\binom{n}{k-1} &= \binom{n+1}{k}
\end{aligned}$$

□

The previous result has triggered the idea of **Pascal's triangle**. This is a triangle formed by numbers. The borders of the triangle have elements equal to 1. The other elements are equal to the sum of the numbers above them. Also, the binomial coefficient $\binom{n}{k}$ appears in the n-th row and (k+1)-th column.

Theorem 1.3 (The Binomial Theorem)**.**

$$
\begin{aligned}
(a+b)^n &= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots \\
&\quad + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n \\
(a+b)^n &= \Sigma_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.
\end{aligned}
$$

Proof. We use proof by mathematical induction.

For $n = 1$,

$$
\begin{aligned}
(a+b)^1 &= \Sigma_{k=0}^{1}\binom{1}{k}a^{1-k}b^k \\
&= \binom{1}{0}a + \binom{1}{1}b \\
&= \frac{1!}{1!0!}a + \frac{1!}{0!1!}b \\
&= 1 \cdot a + 1 \cdot b \\
&= a + b.
\end{aligned}
$$

Let $(a+b)^m = \Sigma_{k=0}^{m}\binom{m}{k}a^{m-k}b^k$ for $m \in \mathbb{Z}$.

Then

$$
\begin{aligned}
(a+b)^{m+1} &= (a+b)(a+b)^m \\
&= (a+b) \cdot \Sigma_{k=0}^{m} \binom{m}{k} a^{m-k} b^k \\
&= a \cdot \Sigma_{k=0}^{m} \binom{m}{k} a^{m-k} b^k + b \cdot \Sigma_{k=0}^{m} \binom{m}{k} a^{m-k} b^k \\
&= \Sigma_{k=0}^{m} \binom{m}{k} a^{m-k+1} b^k + \Sigma_{k=0}^{m} \binom{m}{k} a^{m-k} b^{k+1} \\
&= a^{m+1} + \Sigma_{k=1}^{m} \binom{m}{k} a^{m-k+1} b^k + b^{m+1} + \Sigma_{k=0}^{m-1} \binom{m}{k} a^{m-k} b^k \\
&\overset{j=k+1}{=} a^{m+1} + \Sigma_{k=1}^{m} \binom{m}{k} a^{m-k+1} b^k + b^{m+1} + \Sigma_{j=1}^{m} \binom{m}{j-1} a^{m-j+1} b^j \\
&= a^{m+1} + \Sigma_{k=1}^{m} \left[\binom{m}{k} a^{m-k+1} + \binom{m}{k-1} \right] a^{m-k+1} b^k + b^{m+1} \\
&\overset{Pascal's theorem}{=} a^{m+1} + \Sigma_{k=1}^{m} \binom{m+1}{k} a^{m-k+1} b^k + b^{m+1} \\
&= \Sigma_{k=0}^{m+1} \binom{m+1}{k} a^{(m+1)-k} b^k.
\end{aligned}
$$

□

Number Theory - MTSC 317
Lecture 3

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

September 11, 2014

1 The Division Algorithm

Theorem 1.1 (The Division Algorithm)**.** *For every two integers m and $n > 0$, there exist unique integers q and r such that*

$$m = nq + r, \text{ where } 0 \leq r < n.$$

The integer q is called the quotient produced when dividing m by n, and r is called the remainder of the division with values $0, 1, ...n - 1$.

Corollary 1.2. *If m and n are integers with $n \neq 0$, there exist unique integers q and r for which*

$$m = nq + r, 0 \leq r < |n|.$$

For example for $m = 22$ and $n = 5$, $22 = 4 \cdot 5 + 2$, therefore $q = 4$ and $r = 2$.

Example 1.1. For the following pairs of integers m, n find the quotient and remainder, when m is divided by n. Then write $m = nq + r$.

a) $m = 59$, $n = 7$
b) $m = -58$, $n = 7$

Answer
a) $q = 8$, $r = 3$, $59 = 7 \cdot 8 + 3$
b) $q = -9$, $r = 5$, $-58 = 7 \cdot (-9) + 5$.

We observe that we can use the floor function to express the quotient q and remainder r:

If $m = nq + r$ with $0 \leq r \leq n - 1$, then
$$q = \lfloor \tfrac{m}{n} \rfloor \text{ and } r = m - n\lfloor \tfrac{m}{n} \rfloor$$

Example 1.2. For the following pairs of integers m, n, find $\lfloor \frac{m}{n} \rfloor$ and $m - n\lfloor \frac{m}{n} \rfloor$.
a) $m = 18$, $n = 7$
b) $m = -18$, $n = 7$.

Answer
a) $\lfloor \frac{m}{n} \rfloor = \lfloor 18/7 \rfloor = 2$, $m - n\lfloor \frac{m}{n} \rfloor = 18 - 7.2 = 4$
b) $\lfloor \frac{m}{n} \rfloor = \lfloor -18/7 \rfloor = -3$, $m - n\lfloor \frac{m}{n} \rfloor = -18 - 7.(-3) = 3$.

In the previous exercise we evaluated the quotient and remainder of divisions. In computer terminology the quotient may be symbolized by **div** and the remainder may be symbolized by **mod**.

That is, if $m = nq + r$, then m **div** $n = q$ and m **mod** $n = r$.

Example 1.3. Determine m **div** n and m **mod** n for the following pairs of integers m, n.
a) $m = 75$, $n = 12$
b) $m = -36$, $n = 5$

Answer
a) 75 **div** $12 = 6$, 75 **mod** $12 = 3$.
b) -36 **div** $5 = -8$, -36 **mod** $5 = 4$.

Example 1.4. Show that $\dfrac{a(a^2+2)}{3} \in \mathbb{Z}, \forall a \in \mathbb{Z}, a \geq 1$.

Answer

Per the Division Algorithm every a can be written as $a = 3q$, or $a = 3q+1$, $a = 3q+2$.

For $a = 3q$, $\dfrac{3q(9q^2+2)}{3} = 9q^3 + 2q \ \in \mathbb{Z}$.

For $a = 3q+1$,

$$\begin{aligned}
&\frac{(3q+1)((3q+1)^2+2)}{3} = \frac{(3q+1)(9q^2+6q+1+2)}{3} \\
&= \frac{(3q+1)(9q^2+6q+3)}{3} = \frac{(3q+1)(3q^2+2q+1)3}{3} \\
&= (3q+1)(3q^2+2q+1) \in \mathbb{Z}.
\end{aligned}$$

For $a = 3q+2$,

$$\begin{aligned}
&\frac{(3q+2)((3q+2)^2+2)}{3} = \frac{(3q+2)(9q^2+12q+4+2)}{3} \\
&= \frac{(3q+2)(9q^2+12q+6)}{3} = \frac{(3q+2)(3q^2+4q+2)3}{3} \\
&= (3q+2)(3q^2+4q+2) \in \mathbb{Z}.
\end{aligned}$$

Number Theory - MTSC 317
Lecture 4

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

September 3, 2014

1 Greatest Common Divisor

Definition 1.1. For integers a and b with $a \neq 0$, we say that a divides b if $b = ac$ for some integer c. We indicate this by writing $a \mid b$. If $a \mid b$ then a is called a factor or divisor of b, and b is called a multiple of a. If a does not divide b, we write $a \nmid b$.

Therefore an integer n is even if and only if $2 \mid n$.

For any two given integers a and b $a \mid b$ is a statement. For example $2 \mid 5$ is a false statement, while $2 \mid 6$ is a true statement.

We will prove some divisibility properties of integers next. We note that to show that $a \mid b$ then we need to show that there is an integer c such that $b = ac$. More frequently used proof methods in such problems are the direct proof and proof by induction.

Theorem 1.2. *Let a, b and c be integers with $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Proof. Assume that $a \mid b$ and $a \mid c$, that is $b = da$ and $c = ea$ for some $d, e \in \mathbb{Z}$. Then $b + c = da + ea = (d + e)a$.

Because $d + e \in \mathbb{Z}$ it follows that $a \mid b + c$. $\square$

Theorem 1.3. *Let a and b be integers with $a \neq 0$. If $a \mid b$, then $a \mid bx$ for every integer x.*

Proof. Let $a \mid b$ for $a, b \in \mathbb{Z}$ and $a \neq 0$. Then $b = ra$ for some integer r.

We multiply both sides with an integer x and get $bx = xra = (xr)a$. Because $xr \in \mathbb{Z}$ this can be written as $a \mid bx$. $\square$

Theorem 1.4. *Let a and b be integers with $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for every two integers x and y.*

Proof. This can be considered to be a generalization of the previous two theorems.

Let $a \mid b$ and $a \mid c$ with $a \neq 0$. It follows that $b = ra$ and $c = sa$ for some $r, s \in \mathbb{Z}$.

Then we have that $bx = rax$ and $cy = say$ for $x, y \in \mathbb{Z}$.

Next, we have that $bx + cy = rax + say \to bx + cy = (rx + sy)a$.

Because $rx + sy$ is an integer it follows that $a \mid bx + cy$. $\square$

Theorem 1.5. *Let a and b be integers with $a \neq 0$ and $b \neq 0$. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. We assume that for two integers a, b with $a \neq 0$ and $b \neq 0$, $a \mid b$ and $b \mid c$.

This means that $b = ra$ and $c = sb$ for some integers r, s.

Therefore $c = sra = (sr)a$ and because sr is an integer, it follows that $a \mid c$. $\square$

Theorem 1.6. *Overall, for integers a, b, c*

1. $a \mid 0$, $1 \mid a$, $a \mid a$.
2. $a \mid 1 \Leftrightarrow a = \pm 1$.
3. $(a \mid b) \wedge (c \mid d) \Rightarrow ac \mid bd$.
4. $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c$.
5. $(a \mid b) \wedge (b \mid a) \Leftrightarrow a = \pm b$.
6. $(a \mid b) \wedge (b \neq 0) \Rightarrow |a| \leq |b|$.
7. $(a \mid b) \wedge (a \neq c) \Rightarrow a|ax + bc$ *for arbitrary* $x, y \in \mathbb{Z}$.

Result 1.7. *For every nonnegative integer n,*

$$3 \mid (n^3 - n).$$

Proof. We proceed by induction.

For $n = 0$, we observe that $0^3 - 0 = 0$, thus $3 \mid 0$.

We assume that $3 \mid (k^3 - k)$ for $k \geq 0$.

We show that $3 \mid (k+1)^3 - (k+1)$.

$$\begin{aligned}
(k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - k - 1 \\
&= k^3 + 3k^2 + 2k \\
&= (k^3 - k) + 3k^2 + 3k \\
&= (k^3 - k) + 3(k^2 + k).
\end{aligned}$$

Because $3 \mid (k^3 - k)$, we have that $k^3 - k = 3s$ for $s \in \mathbb{Z}$.
Therefore

$$\begin{aligned}
(k+1)^3 - (k+1) &= 3s + 3(k^2 + k) \\
&= 3(k^2 + k + s).
\end{aligned}$$

Based on fundamental properties of integers it follows that $k^2 + k + s$ is an integer, thus $3 \mid (k+1)^3 - (k+1)$.

By the principle of mathematical induction it follows that $3 \mid (n^3 - n)$. $\square$

Result 1.8. *For every nonnegative integer n,*
$$4 \mid (5^n - 1).$$

Proof. We proceed by induction.

For $n = 0$, we observe that $5^0 - 1 = 1 - 1 = 0$ and $4 \mid 0$.

Next, we assume that $4 \mid (5^k - 1)$ for $k \in \mathbb{Z}$ with $k \geq 0$.

We show that $4 \mid (5^{k+1} - 1)$. We have that $5^{k+1} - 1 = 5^k 5 - 1$. Because $4 \mid (5^k - 1)$, it follows that $5^k - 1 = 4r$ for some $r \in \mathbb{Z}$. Thus $5^k = 4r + 1$. Then

$$\begin{aligned} 5^{k+1} - 1 = 5^k 5 - 1 &= (4r+1)5 - 1 \\ &= 20r + 5 - 1 \\ &= 20r + 4 \\ &= 4(5r+1). \end{aligned}$$

Since $5r + 1$ is an integer, it follows that $4 \mid (5^{k+1} - 1)$.

By the principle of mathematical induction it follows that $4 \mid (5^n - 1)$. $\square$

Theorem 1.9. *Let n be an integer. Then $3 \mid n^2$ if and only if $3 \mid n$.*

Proof. Because the statement is a biconditional we have to prove the following two statements

a) if $3 \mid n$ then $3 \mid n^2$.
b) if $3 \mid n^2$ then $3 \mid n$.

To show a) we assume that $3 \mid n$, therefore $n = 3k$ for some integer k. It follows that $n^2 = (3k)^2 = 3(3k^2)$. Because $3k^2$ is an integer, it follows that $3 \mid n^2$.

For the second statement we will use proof by contrapositive to show that if $3 \nmid n$ then $3 \nmid n^2$.

Let $3 \nmid n$. Then $n = 3q + r$ for some integers q and r.

The remainder r can be 1 or 2.

Case 1: $r = 1$. Then $n = 3q + 1$ and

$$\begin{aligned} n^2 &= (3q+1)^2 \\ &= 9q^2 + 6q + 1 \\ &= 3(3q^2 + 2q) + 1. \end{aligned}$$

Because $3q^2 + 2q$ is an integer, $3 \nmid n^2$.

Case 2: $r = 2$. Then $n = 3q + 2$ and

$$\begin{aligned} n^2 &= (3q+2)^2 \\ &= 9q^2 + 12q + 4 \\ &= 3(3q^2 + 4q + 1) + 1. \end{aligned}$$

Since $3q^2 + 4q + 1$ is an integer, $3 \nmid n^2$. □

Definition 1.10 (Common Divisor)**.** Let a, b, d be integers, where a and b are not both 0 and $d \neq 0$. The integer d is a common divisor of a and b if $d \mid a$ and $d \mid b$.

Definition 1.11 (Greatest Common Divisor)**.** For integers a and b not both 0, the greatest common divisor of a and b is the greatest positive integer that is a common divisor of a and b. The number is denoted by $\gcd(a, b)$.

Example 1.1. Determine by observation the greatest common divisor of each of the following pairs a, b of integers.
(a) $a = 15$, $b = 25$, (b) $a = 16$, $b = 80$
(c) $a = -14$, $b = -18$, (d) $a = 0$, $b = 6$

Answer
(a) $\gcd(15, 25) = 5$, (b) $\gcd(16, 80) = 16$
(c) $\gcd(-14, -18) = 2$, (d) $\gcd(0, 6) = 6$

From the previous example we observe the following:

1. $\gcd(a, b) = \gcd(|a|, |b|)$
2. $\gcd(a, 0) = |a|$
3. if $a, b \neq 0$ and $a \mid b$, then $\gcd(a, b) = a$.

Theorem 1.12. *Given integers a and b not both of which are zero, there exist integers x and y such that $gcd(a, b) = ax + by$.*

Definition 1.13 (Relatively Prime Integers)**.** Two integers a and b not both 0, are relatively prime if $\gcd(a, b) = 1$.

Theorem 1.14. *Let a and b be integers not both zero. Then a and b are relatively prime iff there exist integers x and y such that $1 = ax + by$.*

Result 1.15. *Every two consecutive positive integers are relatively prime.*

Proof. Let n and $n+1$ be consecutive positive integers and let $d = \gcd(n, n+1)$.

Hence $d \mid n$ and $d \mid n+1$. This means that $n = dr$ and $n + 1 = ds$ for some integers d and s.

Based on these two relations, $dr + 1 = ds \to 1 = ds - dr \to 1 = d(s - r)$.

Because $s - r$ is an integer, $d \mid 1$, therefore $d \leq 1$. Also, $d \geq 1$, so $d = 1$. $\square$

Corollary 1.16. *If $a \mid c$ and $b \mid c$ with $gcd(a, b) = 1$, then $ab \mid c$.*

Theorem 1.17. *Let a and b be integers not both zero. A positive integer d is $gcd(a, b)$ iff*

1. *$d \mid a$ and $d \mid b$*
2. *if $c \mid a$ and $c \mid b$, then $c \mid d$.*

Theorem 1.18 (Euclid's Lemma)**.** *If $a \mid bc$ with $gcd(a, b) = 1$, then $a \mid c$.*

Number Theory - MTSC 317
Lecture 5

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

September 10, 2014

1 The Euclidean Algorithm

Theorem 1.1. *Let a and b be two positive integers. If $b = aq + r$ for some integers q and r, then*

$$gcd(a, b) = gcd(r, a).$$

Let $a < b$ in the previous theorem. If we also assume that q is the quotient and r is the remainder, when b is divided by a, then

$$\gcd(a, b) = \gcd(r, a), \text{ with } 0 \leq r < b.$$

Now if $r = 0$ then $\gcd(a, b) = \gcd(0, a) = a$.

If $r \neq 0$, then we continue and divide a by r with remainder r_2, so $gcd(r, a) = gcd(r_2, r)$. We continue this until we reach a remainder equal to 0.

$$\gcd(a, b) = \gcd(r, a) = gcd(r_2, r) = gcd(r_3, r_2) = ... = \gcd(0, r_k) = r_k.$$

Therefore, the greatest common divisor of a and b is the last nonzero remainder obtained when the sequence of divisions described above is performed. This method for determining $\gcd(a, b)$ is called the Euclidean algorithm.

Example 1.1. Use the Euclidean algorithm to find $\gcd(384, 477)$.

Answer We recursively apply the Euclidean algorithm to the remainder of each division as follows.

$$\begin{aligned}
477 \quad \bmod 384 &= 93 \\
384 \quad \bmod 93 &= 12 \\
93 \quad \bmod 12 &= 9 \\
12 \quad \bmod 9 &= 3 \\
9 \quad \bmod 3 &= 0.
\end{aligned}$$

Therefore $\gcd(384, 477) = 3$.
Represent 3 as a linear combination of 384 and 477.

$$\begin{aligned}
3 &= 12 - 9 \\
&= 12 - (93 - 7 \cdot 12) \\
&= -93 + 8 \cdot 12 \\
&= -93 + (8 \cdot (384 - 4 \cdot 93)) \\
&= -93 + 8 \cdot 384 - 32 \cdot 93 \\
&= 8 \cdot 384 - 33 \cdot 93 \\
&= 8 \cdot 384 - 33 \cdot (477 - 384) \\
&= 41 \cdot 384 - 33 \cdot 477
\end{aligned}$$

Theorem 1.2. *If $k > 0$, then $gcd(ka, kb) = k \cdot gcd(a, b)$.*

Proof. $gcd(ka, kb)$ is the smallest integer of the form $kax + kby$, which is $k \cdot (ax + by)$, hence it is $k \cdot gcd(a, b)$. □

Example 1.2. Find $gcd(428, 14)$.

Answer
Based on previous theorem, $gcd(428, 14) = 2 \cdot gcd(214, 7)$.
We now use the Euclidean algorithm to find $gcd(214, 7)$:

$$\begin{aligned}
214 &= 30 \cdot 7 + 4 \\
7 &= 1 \cdot 4 + 3 \\
4 &= 1 \cdot 3 + 1 \\
3 &= 3 \cdot 1
\end{aligned}$$

$\therefore gcd(214, 7) = 1 \therefore gcd(428, 14) = 2 \cdot gcd(214, 7) = 2$.

2 Least Common Multiples

Definition 2.1. For two positive integers a and b, an integer n is a common multiple of a and b if n is a multiple of a and b. The smallest positive integer that is a common multiple of a and b is the least common multiple of a and b. The number is denoted by $\text{lcm}(a, b)$ and has the following properties:

1. $a \mid n$ and $b \mid n$.
2. If $a \mid c$ and $b \mid c$, then $c \geq n$.

Example 2.1. Determine by observation the least common multiple of a and b.
(a) $a = 6$ $b = 9$, (b) $a = 10$ $b = 10$,
(c) $a = 5$ $b = 7$, (d) $a = 15$ $b = 30$,

Answer
(a) $\text{lcm}(6, 9) = 18$, (b) $\text{lcm}(10, 10) = 10$
(c) $\text{lcm}(5, 7) = 35$, (d) $\text{lcm}(15, 30) = 30$

Theorem 2.2. *For every two positive integers a and b,*
$$ab = \gcd(a, b)lcm(a, b)$$

Example 2.2. Find $lcm(92, 16)$ using Theorem 2.2.

Answer First, find $gcd(92, 16)$:

$$\begin{aligned}
92 &= 5 \cdot 16 + 12 \\
16 &= 1 \cdot 12 + 4 \\
12 &= 3 \cdot 4
\end{aligned}$$

Therefore $gcd(92, 16) = 4$. Because of Theorem 2.2, $gcd(92, 16) \cdot lcm(92, 16) = 92 \cdot 16 \therefore lcm(92, 16) = \dfrac{92 \cdot 16}{gcd(92, 16)} = \dfrac{92 \cdot 16}{4} = 92 \cdot 4 = 368$.

3 Linear Combinations of Integers

Definition 3.1. Let a and b be two integers. An integer of the form $ax+by$, where x and y are integers, is a linear combination of a and b.

Theorem 3.2. *Let a and b be integers that are not both 0. Then $gcd(a,b)$ is the smallest positive integer that is a linear combination of a and b.*

Example 3.1. For each of the following pairs of integers, express $d = \gcd(a,b)$ as a linear combination of a and b.
(a) $a = 10$ $b = 14$, (b) $a = 12$ $b = 12$
(c) $a = 18$ $b = 30$, (d) $a = 25$ $b = 27$

Answer
(a) $\gcd(10,14) = 2 = 10 \cdot 3 + 14 \cdot (-2)$
(b) $\gcd(12,12) = 12 = 12 \cdot 1 + 12 \cdot 0$
(c) $\gcd(18,30) = 6 = 18 \cdot 2 + 30 \cdot (-1)$
(d) $\gcd(25,27) = 1 = 25 \cdot 13 + 27 \cdot (-12)$

We can solve (d) using the Euclidean algorithm
$27 = 25 \cdot 1 + 2 \rightarrow 2 = 27 - 25 \cdot 1$
$25 = 12 \cdot 2 + 1 \rightarrow 1 = 25 - 12 \cdot 2$
Therefore

$$\begin{aligned} 1 &= 25 - 12 \cdot (27 - 25 \cdot 1) \\ &= 25 - 12 \cdot 27 + 12 \cdot 25 \\ &= 13 \cdot 25 - 12 \cdot 27 \end{aligned}$$

Corollary 3.3. *Let a and b be integers that are not both 0 and let $d = gcd(a,b)$. If n is an integer that is a common divisor of a and b then $n \mid d$.*

Proof. Based on theorem 3.2 $d = ax + by$ for some integers x, y.
Also $n \mid a$ and $n \mid b$, therefore $a = nq$ and $b = nr$ for some integers q and r.
So $d = ax + by = nqx + nry = n(qx + ry)$.
Because $qx + ry$ is an integer, $n \mid d$. □

Corollary 3.4. *Two integers a and b are relatively prime if and only if 1 is a linear combination of a and b; that is, gcd$(a, b) = 1$ if and only if $ax + by = 1$ for some integers x and y.*

Example 3.2. Use Corollary 3.4 to show that the following pairs are relatively prime.

(a) every two consecutive integers

(b) every two odd integers that differ by 2.

Answer

(a) Let $n \in \mathbb{Z}$ and the consecutive integer $n + 1$.

Because $(-1) \cdot n + n + 1 = 1$.

By the Corollary 3.4 it follows that $\gcd(n, n + 1) = 1$ and $m - n = 2$.

(b) Let an odd integer m such that $m = 2k + 1$ and an odd integer $n = m + 2 = 2k + 1 + 2 = 2k + 3$ with $k \in \mathbb{Z}$.

Since $1 = (2k + 1)(k + 1) + (2k + 3)(-k)$, by the Corollary 3.4 it follows that $\gcd(m, n) = 1$.

Theorem 3.5. *Let a, b and c be integers with $a \neq 0$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Let $a \mid bc$. Then $bc = qa$ for some integer q.

Because $\gcd(a, b) = 1$, by the Corollary 3.4 it follows that $ax + by = 1$ for some integers a and b.

Therefore $c = c \cdot 1 = c(ax + by) = cax + cby = cax + qay = a(cx + qy)$.

Because $cx + qy$ is an integer, it follows that $a \mid c$. $\square$

Corollary 3.6. *Let b and c be integers and let p be a prime. If $p \mid bc$, then either $p \mid b$ or $p \mid c$.*

Theorem 3.7. *Let $a_1, a_2, ..., a_n$ be $n \geq 2$ integers and let p be a prime. If*

$$p \mid a_1 a_2 ... a_n,$$

then $p \mid a_i$ for some integer i with $1 \leq i \leq n$.

Theorem 3.8 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ is either prime or can be expressed as a product of (not necessarily distinct) primes, that is,*

$$n = p_1 p_2 ... p_k,$$

where $p_1, p_2, ..., p_k$ are primes. This factorization is unique except possibly for the order in which the primes appear.

Number Theory - MTSC 317
Lecture 6

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

September 22, 2014

1 The Diophantine Equation

We use the term 'Diophantine Equation' to refer to an equation to be solved in the integer space.

The simplest of these equations is a linear equation in two unknowns, that is $ax + by = c$, where a, b, c are integers and a, b are not both zero.

Theorem 1.1. *The linear Diophantine equation $ax + by = c$ has a solution iff $d \mid c$, where $d = \gcd(a, b)$. If x_0, y_0 is one solution of the equation, then all other solutions are given by:*

$$x = x_0 + \left(\frac{b}{d}\right) t, \quad y = y_0 - \left(\frac{a}{d}\right) t$$

where t is an arbitrary integer.

Example 1.1. Consider the linear Diophantine equation

$$172x + 20y = 1000.$$

We first find the $\gcd(172, 20)$:

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 \end{aligned}$$

Therefore $\gcd(172, 20) = 4$.
Because $\gcd(172, 20) \mid 1000$, the Diophantine equation has a solution.
We next find $\gcd(172, 20)$ as a linear comination of 172 and 20.

$$\begin{aligned} 4 &= 12 - 8 \\ 4 &= 12 - (20 - 12) \\ 4 &= 2 \cdot 12 - 20 \\ 4 &= 2 \cdot (172 - 8 \cdot 20) - 20 \\ 4 &= 2 \cdot 172 - 17 \cdot 20 \end{aligned}$$

Then

$$\begin{aligned} 1000 &= 250 \cdot 4 = 250 \cdot (2 \cdot 172 - 17 \cdot 20) \\ 1000 &= 500 \cdot 172 - 4250 \cdot 20 \end{aligned}$$

Hence, one solution is $x_0 = 500, \quad y_0 = -4250$.
According to the above theorem, the set of solutions is given by:

$$x = 500 + 5t \quad y = -4250 - 43t.$$

To find positive solutions we further require that

$$500 + 5t > 0, \quad -4250 - 43t > 0$$

$$t > -100, \quad t < \frac{-4250}{43}$$

$$-100 < t < -98\frac{36}{43}$$

$$\therefore t = -99 \text{ for positive solution.}$$

$$\therefore x = 5, \quad y = 7.$$

Corollary 1.2. *If* $\gcd(a, b) = 1$ *and if* x_0, y_0 *is a particular solution of the linear Diophantine equation* $ax + by = c$*, then all solutions are given by*

$$x = x_0 + bt, \quad y = y_0 - at.$$

for integral values of t*.*

For example, the equation $5x + 22y = 18$, where $\gcd(5, 22) = 1$ has a solution $x_0 = 8, \quad y_0 = -1$. Then the set of solutions is given by

$$x = 8 + 22t, \quad y = -1 - 5t.$$

for an arbitrary integer t.

Number Theory - MTSC 317
Lecture 7

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

September 21, 2014

1 Primes

Definition 1.1. A prime is an integer $p \geq 2$ whose only positive integer divisors are 1 and p.

Some prime numbers are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Theorem 1.2. *If p is a prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Proof. The strategy is to divide the proof into the cases $p \mid a$ and $p \nmid a$. $\square$

Corollary 1.3. *If p is a prime and $p \mid a_1, a_2, \ldots, a_n$, then $p \mid a_k$ for some $1 \leq k \leq n$, $k \in \mathbb{Z}$.*

Proof. The strategy is to utilize mathematical induction and the previous result. $\square$

Corollary 1.4. *If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid q_1, q_2, \ldots, q_n$, then $p = q_k$ for some $1 \leq k \leq n$, $k \in \mathbb{Z}$.*

Proof. The strategy is to utilize previous corollary and the definition of prime numbers. $\square$

1.1 The Fundamental Theorem of Arithmetic

Theorem 1.5 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ is either prime or can be expressed as a product of (not necessarily distinct) primes, that is,*

$$n = p_1 p_2 ... p_k,$$

where $p_1, p_2, ..., p_k$ are primes. This fatorization is unique except possibly for the order in which the primes appear.

Example 1.1.

In some cases we can check if a prime p divides an integer n.

- 2 divides n only if n is even. The last digit of an even number must be even.
- $4 = 2^2$ divides n if the last two digits of n are divided by 4. For example, $4 \mid 6912$ because $4 \mid 12$.
- 3 divides an integer n if and only if 3 divides the sum of the digits of n. For example $3 \mid 324$ because $3 \mid (3 + 2 + 4)$.
- $9 = 3^2$ divides n if and only if 9 divides the sum of the digits of n.
- 5 divides n if the last digit of n is 5 or 0.
- There is a method for finding if an integer n can be divided by 11. Let a the sum of alternating digits of n, and b the sum of the remaining digits. Then $11 \mid n$ if and only if $11 \mid (a - b)$. For example, $11 \mid 9,775,887$ because $11 \mid ((9 + 7 + 8 + 7) - (7 + 5 + 8))$, $11 \mid (31 - 20)$.

Corollary 1.6. *Any positive integer $n > 1$ can be written uniquely in a canonical form*

$$n = {p_1}^{k_1} {p_2}^{k_2} \dots {p_r}^{k_r}$$

where, for $i = 1, 2, \dots, r$ $k_i \in \mathbb{Z}$ and p_i is a prime with $p_1 < p_2 < \dots < p_r$.

Example 1.2. Canonical forms:

$$360 = 2^3 \cdot 3^3 \cdot 5$$

$$17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

Note: Prime factorizations can be used to find the gcd of two numbers.

Theorem 1.7 (Attributed to Pythagoras)**.** *The number $\sqrt{2}$ is irrational.*

Proof. Proof strategy: use proof by contradiction by assuming that $\sqrt{2}$ is rational. $\square$

Number Theory - MTSC 317
Lecture 8

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

August 30, 2015

1 The Sieve of Eratosthenes

We can determine if an integer n is prime or composite can be done by checking if n can be divided by all smaller positive integers.

This process can become very tedious for large integers.

We can reduce the workload by use of the following result:

Corollary 1.1. *If n is a composite number, then n has a prime factor p such that $p \leq \sqrt{n}$.*

Proof. Let n be a composite number. Then by definition $n = ab$ for some integers a, b with $1 < a < n$ and $1 < b < n$. Suppose that $a < b$. Then $a^2 < ab = n$, thus $a < \sqrt{n}$. Because $a \geq 2$ according to the Fundamental Theorem of Arithmetic there is some prime number p such that $p \mid a$ and so $p \leq a < \sqrt{n}$. According to previously proved theorem $p \mid ab$, that is $p \mid n$. $\square$

We can use this corollary to find out if an integer is a prime.

Example 1.1. Show that 103 is a prime.

Answer We check if there are any primes lower than $\sqrt{103}$ that divide 103. We observe that $10 < \sqrt{103} < 11$, so we check the primes 2, 3, 5, 7. We observe that none of them is a factor of 103, therefore 103 is a prime number.

Example 1.2. Determine if 509 is a prime.

Answer We have that $22 < \sqrt{509} < 23$. We find primes smaller than 22. These are 2, 3, 7, 9, 11, 13, 17, 19.

None of these numbers is a divisor of 509.

Therefore 509 is a prime integer.

The **Sieve of Eratosthenes** is a smart technique for finding primes smaller than a given integer n. We first write down an ordered list of integers 2 to n. We then eliminate all multiples $2p, 3p, \ldots$ of primes $p \leq \sqrt{n}$. The remaining integers, that is the numbers that do not fall through the sieve, are primes.

1.1 There are Infinitely Many Primes

Theorem 1.2. *There are infinitely many primes.*

Proof. We will use proof by contradiction.

We assume that there is a finite number of primes, $p_1, p_2, ..., p_k$.

Let $n = p_1 p_2 ... p_k + 1$. Because n is greater than each prime, n must be composite. By the fundamental theorem of arithmetic, at least one prime must divide n say $p_j \mid n$. Therefore $n = p_j r$ for some integer r. That means

$$\begin{aligned} p_1 p_2 ... p_k + 1 &= p_j r \\ p_1 p_2 ... p_{j-1} p_j p_{j+1} ... p_k + 1 &= p_j r \\ 1 &= p_j r - p_1 p_2 ... p_{j-1} p_j p_{j+1} ... p_k \\ 1 &= p_j (r - p_1 p_2 ... p_{j-1} p_{j+1} ... p_k) \end{aligned}$$

We observe that $r - p_1 p_2 ... p_{j-1} p_{j+1} ... p_k + 1$ is an integer, hence $p_j \mid 1$. This is a contradiction because a prime number is by definition greater than 2. □

Theorem 1.3. *If p_n is the $n-th$ prime number, then $p_n \leq 2^{2^{n-1}}$.*

Proof. Strategy: use Mathematical Induction. □

Corollary 1.4. *For $n \geq 1, \exists n+1$ primes less than 2^{2^n}*

Proof. Using above theorem it follows that $p_1, p_2, \dots p_{n+1}$ are all smaller than or equal to 2^{2^n}. $\square$

Theorem 1.5 (The Prime Number Theorem)**.** *The number $\pi(n)$ is approximately equal to $n/\ln n$. More specifically*

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1.$$

Special forms of primes are numbers written as a string of 1s, for example 11, 111, 11111, that we call **repunits** and symbolize by R_n, where n is the number of digits. For these numbers we have that $R_n = \dfrac{10^n - 1}{9}$.

1.2 Unsolved Problems Involving Primes

1. Two positive integers p and $p + 2$ are called twin primes if they are both primes, for example, 5 and 7 are twin primes. The **two primes conjecture** is that there are infinitely many twin primes.

2. **Goldbach's Conjecture:** Every even integer that is 4 or more can be expressed by the sum of two primes.

3. Observe that the following Fibonacci numbers are primes: 2, 3, 5, 13. Are there infinitely many prime Fibonacci numbers?

Number Theory - MTSC 317
Lecture 9

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 15, 2014

1 Congruence

In several occasions we are interested in the parity of integers. We noticed that two integers are both even if both have a remainder 0 when divided by 2. Also, two integers are odd if they both have a remainder 1 when divided by 2.

In this section we deal with numbers that have the same remainder when divided by an integer n with $n \geq 2$. We begin with a definition of congruence and reach this observation.

Definition 1.1. For integers a, b and $n \geq 2$, the integer a is congruent to b modulo n if $n \mid (a - b)$.

To show that a is congruent to b modulo n we use the notation $a \equiv b(\mod n)$. To show that a is not congruent to b modulo n we write $a \not\equiv b(\mod n)$.

Example 1.1. We observe that
$47 \equiv 5(\mod 7)$, because $7 \mid (47 - 5)$.
$93 \equiv 84(\mod 9)$, because $9 \mid (93 - 84)$.
$58 \not\equiv 47(\mod 6)$, because $6 \mid (58 - 47)$.

Theorem 1.2. *Let a, b and $n \geq 2$ be integers. Then $a \equiv b(\mod n)$ if and only if $a = b + kn$ for some integer k.*

Proof. This is a biconditional so we need to prove two statements.

We first show that if $a \equiv b(\mod n)$, then $a = b + kn$ for some integer k.
Let $a \equiv b(\mod n)$ for $a, b, n \in \mathbb{Z}$ with $n \geq 2$.
Then according to the definition $n \mid (a - b)$.
Hence, $a - b = nk$ for some integer k and $a = b + nk$.

Next, we show that if $a = b + kn$, then $a \equiv b(\mod n)$.
We assume that $a = b + kn$ for an integer k.
Then $a - b = kn$, therefore $n \mid (a - b)$.
By definition this means that $a \equiv b(\mod n)$. □

Theorem 1.3. *Let a, b and $n \geq 2$ be integers. Then $a \equiv b(\mod n)$ if and only if a and b have the same remainder when divided by n.*

Proof. This is a biconditional so we need to prove two statements.

First, we show that if a and b have the same remainder when divided by n, then $a \equiv b(\mod n)$.

Let a and b have the same remainder $r > 0, r \in \mathbb{Z}$ when divided by n.

Therefore, $a = nk_1 + r$ and $b = nk_2 + r$, for $k_1, k_2 \in \mathbb{Z}$.

We have that $a - b = nk_1 + r - (nk_2 + r) = nk_1 + r - nk_2 - r = nk_1 - nk_2 = n(k_1 - k_2)$.

Because $k_1 - k_2$ is an integer, $n \mid (a - b)$.

We also need to show that if $a \equiv b(\mod n)$, then a and b have the same remainder when divided by n.

We use proof by contrapositive.

We assume that a and b have different remainders when divided by n.

Hence, $a = k_1 n + r_1$ and $b = k_2 n + r_2$ with $r_1 \neq r_2$.

We will show that $a \not\equiv b(\mod n)$.

Then $a - b = k_1 n + r_1 - (k_2 n + r_2) = k_1 n + r_1 - k_2 n - r_2 = (k_1 - k_2)n + (r_1 - r_2)$.

Because $r_1 \neq r_2 \rightarrow r_1 - r_2 \neq 0$, therefore $n \nmid (a - b)$. This means that $a \not\equiv b(\mod n)$. □

Corollary 1.4. *Let a, b and $n \geq 2$ be integers. Then $a \equiv b(\mod n)$ if and only if*

$$a \mod n = b \mod n.$$

Example 1.2. Use Corollary 1.4 to determine whether the following pairs of integers a, b for integer $n \geq 2$ are $a \equiv b(\mod n)$.

(a) $a = 31$, $b = 47$, $n = 3$.

(b) $a = 35$, $b = 59$, $n = 6$.

Answer

(a) We observe that $31 \mod 3 = 1$ and $47 \mod 3 = 2$. Because $31 \mod 3 \neq 47 \mod 3$, it follows by Corollary 1.4 that $31 \not\equiv 47(\mod 3)$.

(b) We observe that $35 \mod 6 = 5$ and $59 \mod 6 = 5$. Because $35 \mod 6 = 59 \mod 6$, it follows by Corollary 1.4 that $35 \equiv 59(\mod 6)$.

Congruence can be considered as a new form of equality as seen below.

Theorem 1.5. *Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. We have that:*

1. $a \equiv a(\mod n)$.
2. *If* $b \equiv a(\mod n)$, *then* $a \equiv b(\mod n)$.
3. *If* $a \equiv b(\mod n)$ *and* $b \equiv d(\mod n)$, *then* $a + c \equiv (b + d)(\mod n)$ *and* $ac \equiv (bd)(\mod n)$.
4. *If* $a \equiv b(\mod n)$ *and* $b \equiv c(\mod n)$, *then* $a \equiv c(\mod n)$.
5. *If* $a \equiv b(\mod n)$, *then* $ac \equiv bc(\mod n)$ *and* $(a + c) \equiv (b + c)(\mod n)$.
6. *If* $a \equiv b(\mod n)$ *and* $a^k \equiv b^k(\mod n)$ *for* $k \in \mathbb{Z}, k > 0$.

Theorem 1.6. *If* $ca \equiv cb(\mod n)$, *then* $a \equiv b(\mod n/d)$, *where* $d = \gcd(c, n)$.

Proof. Proof strategy: Let $n \mid c(a - b)$. Use $\gcd(c, n)$ properties. □

Corollary 1.7. *If* $ca \equiv cb(\mod n)$ *and* $\gcd(c, n) = 1$, *then* $a \equiv b(\mod n)$.

Corollary 1.8. *If* $ca \equiv cb(\mod n)$ *and* $p \nmid c$, *where* p *is prime, then* $a \equiv b(\mod p)$.

Proof. Because p is prime and $p \nmid c$, we have that $\gcd(c, p) = 1$. Result follows from previous theorem. □

Number Theory - MTSC 317
Lecture 10

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 19, 2014

1 Binary and Decimal Representations of Integers

Result 1.1. *Given an integer $b > 1$, any positive integer N can be written uniquely in terms of powers of b as $N = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_2 b^2 + a_1 b + a_0$ where the coefficients a_k can take on the values $0, 1, 2, \ldots, b-1$.*

Proof. Proof strategy: use the Division algorithm recursively to show the polynomial representation. Then use proof by contradiction to show uniqueness. □

Hence, any integer N can be uniquely represented by the coefficients a_i and base integer b, $i = 0, 1, \ldots, m$: $N = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_2 b^2 + a_1 b + a_0$.

A simpler representation is $(a_m a_{m-1} \ldots a_0)_b$.

This is called base b place-value notation for N.

For $b = 2$, we have the binary system.

For $b = 10$, we have the decimal system.

Example 1.1.

$$
\begin{aligned}
(121)_{10} &= 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\
&= (1111001)_2 \\
(10101)_2 &= 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\
&= 16 + 4 + 1 = 21.
\end{aligned}
$$

Binary representation is more suitable for electronic devices, based on closed or open switch.

The binary exponential algorithm: to calculate the value $a^k(\mod n)$ for large k we follow these steps:

1. write exponent in binary form $k = (a_m a_{m-1} \dots a_1 a_0)_2$
2. calculate $a^{2j}(\mod n)$, corresponding to 1s in binary form
3. multiply previous terms together and get final result.

Example 1.2. Calculate $5^{113}(\mod 131)$.

1. Binary form of exponent

   $113 = 64 + 32 + 16 + 1 = (1110001)_2$

2. Obtain $5^{2j}(\mod 131)$

$$
\begin{aligned}
5^1 &\equiv 5(\mod 131) \\
5^2 &\equiv 25(\mod 131) \\
5^4 &\equiv 25^2(\mod 131) \equiv 101(\mod 131) \\
5^8 &\equiv 101^2(\mod 131) \equiv 114(\mod 131) \\
5^{16} &\equiv 114^2(\mod 131) \equiv 27(\mod 131) \\
5^{32} &\equiv 27^2(\mod 131) \equiv 74(\mod 131) \\
5^{64} &\equiv 74^2(\mod 131) \equiv 105(\mod 131)
\end{aligned}
$$

3. $5^{113} = 5^{64+32+16+1} = 5^{64} 5^{32} 5^{16} 5^1 \equiv 105 \cdot 74 \cdot 27 \cdot 5 \equiv 33(\mod 131)$.

Theorem 1.2. *Let $P(x) = \Sigma_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b(\mod n)$, then $P(a) = P(b)(\mod n)$.*

Definition 1.3. If $P(x)$ is a polynomial with integral coefficients, we say that a is a solution of the congruence $P(x) \equiv 0(\mod n)$ if $P(a) \equiv 0(\mod n)$.

Theorem 1.4. *If a is a solution of $P(x) \equiv 0(\mod n)$ and $a \equiv b(\mod n)$, then b is also a solution.*

Proof. From last theorem $P(a) = P(b)(\mod n) \therefore P(b) = P(a)(\mod n)$.

Because $P(a) \equiv 0(\mod n)$ and $P(b) = P(a)(\mod n)$, $P(b) \equiv 0(\mod n)$. □

Theorem 1.5. *Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0$ be the decimal expression of the integer N, $N > 0$, $0 \leq a_k < 10$ and let $S = a_0 + a_1 + \ldots + a_m$. Then $9 \mid N \iff 9 \mid S$.*

Proof. Let $P(x) = \Sigma_{k=0}^{m} a_k \cdot x^k$ with integral coefficients.

Then $P(10) = N$ and $P(1) = S$.

We have that $10 \equiv 1(\mod 9)$ and $1 \equiv 1(\mod 9)$.

Previous theorem $\therefore P(10) \equiv P(1)(\mod 9) \therefore N \equiv S(\mod 9)$.

Let $9 \mid N \therefore N \equiv 0(\mod 9) \therefore S \equiv 0(\mod 9) \therefore 9 \mid S$.

Let $9 \mid S \therefore S \equiv 0(\mod 9) \therefore N \equiv (\mod 9) \therefore 9 \mid N$. □

Theorem 1.6. *Let* $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0$ *be the decimal expression of the integer* N, $N > 0$, $0 \leq a_k < 10$ *and let* $S = a_0 - a_1 + \ldots + (-1)^m a_m$. *Then* $11 \mid N \iff 11 \mid S$.

Proof. Proof strategy: we let $P(x) = \Sigma_{k=0}^{m} a_k \cdot x^k$ with integral coefficients and observe that $10 \equiv (-1)(\mod 11)$. Then continue proof as in previous theorem.

□

Number Theory - MTSC 317
Lecture 11

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 24, 2014

1 Linear Congruences and the Chinese Remainder Theorem

An equation of the form $ax \equiv (\mod n)$ is called a linear congruence. A solution of this equation type is an integer x_0 for which $ax_0 \equiv (\mod n)$. We have that $ax_0 \equiv (\mod n) \leftrightarrow ax_o - b = ny_0$ for some integer y_0.

So our problem becomes that of finding all solutions of the linear Diophantine equation

$$ax_0 - ny_0 = b.$$

Theorem 1.1. *The linear congruence $ax \equiv (\mod n)$ has a solution iff $d \mid b$, where $d = \gcd(a, n)$. If $d \mid b$ the equation has d mutually incongruent solutions modulo n.*

Proof. Proof strategy: Use theorem for solutions of linear Diophantine equations. Use proof by contradiction to show that solutions are incongruent modulo n. □

If x_0 is any solution of $ax \equiv b(\mod n)$ then the $d = \gcd(a, n)$ solutions are given by $x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$.

Corollary 1.2. *If* $\gcd(a, n) = 1$*, then the linear congruence* $ax \equiv b(\mod n)$ *has a unique solution modulo* n*.*

Example 1.1. Find the solutions, if any, of $18x \equiv 30(\mod 42)$.

We have that $gcd(18, 42) = 6$.

Then $6 \mid 30$, hence we have 6 solutions given by

$$\begin{aligned} x \equiv & x_o + \frac{42}{6} \cdot t, \quad t = 0, \ldots, 5 \\ \equiv & x_o + 7 \cdot t. \end{aligned}$$

One solution is $x = 4$, *hence*

$$x \equiv 4, 11, 18, 25, 32, 39, 46(\mod 42).$$

Example 1.2. Solve the linear equation

$$9x \equiv 21(\mod 30).$$

First, $d = \gcd(9, 30) = 3$.

Because $3 \mid 21$ we have 3 solutions.

We have to solve the equivalent Diophantine equation $9x - 30y = 21$. We use the Euclidean algorithm to express $3 = 9 \cdot k + 30 \cdot j$.

$$\begin{aligned} 30 &= 3 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

Next we find a solution to the Diophantine equation.

$$\begin{aligned} 3 &= 30 - 3 \cdot 9 \\ 21 &= 30 \cdot 7 + 9 \cdot (-21) \\ 21 &= 9 \cdot (-21) + (-30) \cdot (-7). \end{aligned}$$

Hence, $x_0 = -21$ and $y_0 = -7$.

The solutions are given by

$$\begin{aligned} x &= -21 + \frac{30}{3} t, \quad t = 0, 1, 2 \\ &= -21 + 10t. \end{aligned}$$

These integers are incongruent modulo 30 and the incongruent solutions are

$$\begin{aligned} x &\equiv -21 \pmod{30} \\ x &\equiv -11 \pmod{30} \\ x &\equiv -1 \pmod{30}, \end{aligned}$$

which can be written as $x \equiv 9, 19, 29 \pmod{30}$.

Theorem 1.3 (Chinese Remainder Theorem)**.** *Let $n_1, n_2, n_3, \ldots, n_r$ be positive integers, such that $\gcd(n_i, n_j) = 1$ for $i \neq j$.*

Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \ldots n_r$.

Proof. Proof strategy: Compute $N_k = \frac{n}{n_k} = n_1 n_2 \ldots n_{k-1} n_{k+1} \ldots n_r$. From $\gcd(N_k, n_k) = 1$, define and solve $N_k x \equiv 1 \pmod{n_k}$. Show that $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r$ is the solution of above system. □

Example 1.3. The problem posed by Sun-Tsu corresponds to the system of congruences:

$$x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}.$$

We have that $n = 3 \cdot 5 \cdot 7 = 105$ and

$$N_1 = \frac{n}{3} = 35, N_2 = \frac{n}{5} = 21, N_3 = \frac{n}{3} = 15.$$

The linear congruences:

$$35x \equiv 1 \pmod 3), 21x \equiv 1 \pmod 5), 15x \equiv 1 \pmod 7),$$

are satisfied by $x_1 = 2, x_2 = 1, x_3 = 1$.
The solution is

$$\begin{aligned} x &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &= 140 + 63 + 30 \\ &= 233. \end{aligned}$$

Modulo 105 we get $x = 233 \equiv 23 \pmod{105}$.

Example 1.4. Solve the linear congruence:

$$17x \equiv 9 \pmod{276}.$$

Because $276 = 3 \cdot 4 \cdot 23$, the equivalent system is

$$17x \equiv 9 \pmod 3), 17x \equiv 9 \pmod 4), 17x \equiv 9 \pmod{23},$$

or,

$$x \equiv 0 \pmod 3), x \equiv 1 \pmod 4), 17x \equiv 9 \pmod{23}.$$

We have that

$$x \equiv 0 \pmod 3) \therefore x = 3k \text{ for } k \in \mathbb{Z}.$$

Then

$$3k \equiv 1 \pmod 4) \therefore k \equiv 9k \equiv 3 \pmod 4), \text{ where } k = 3 + 4j, j \in \mathbb{Z}.$$

Also

$$x = 3(3 + 4j) = 9 + 12j.$$

Based on the previous results we have that

$$17(9 + 12j) \equiv 9 \pmod{23} \therefore 153 + 204j \equiv 9 \pmod{23}$$
$$\therefore 204j \equiv -144 \pmod{23} \therefore 3j \equiv 6 \pmod{23} \therefore j \equiv 2 \pmod{23}$$
$$\therefore j = 2 + 23t, t \in \mathbb{Z}.$$

Finally

$$x = 9 + 12(2 + 23t) = 9 + 24 + 276t = 33 + 276t.$$

That is, $x \equiv 33 \pmod{276}$ is a solution to the system of congruences and the original linear congruence.

Number Theory - MTSC 317
Lecture 12

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 5, 2014

1 Fermat's Little Theorem and Pseudoprimes

Definition 1.1 (Fermat's Little Theorem)**.** Let p be a prime and let $p \nmid a$. Then $a^{p-1} \equiv 1 (\mod p)$.

Proof. Let a prime p and let $p \nmid a$. We take the first $p-1$ multiples of a: $a, 2a, \ldots, (p-1)a$.

These numbers are not congruent modulo p to each other, nor is any congruent to 0.

Indeed, let $ra \equiv sa (\mod p)$ for some $0 < s \leq r < p$ with $s, r \in \mathbb{Z}$.

Then $r \equiv s (\mod p) \therefore p \mid r - s$.

This is not possible because both r and s are smaller than p, hence $r - s < p$.

Therefore the $p-1$ multiples of a must be congruent modulo p to $1, 2, 3, \ldots, p-1$ in some order.

After multiplying them all we get

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

□

Corollary 1.2. *If p is a prime, then $a^p \equiv a(\mod p), \forall a \in \mathbb{Z}$.*

Proof. *Case 1:* Let $p \mid a$. Then

$$a \equiv 0(\mod p) \therefore a^p \equiv 0 \equiv a(\mod p).$$

Case 2: Let $p \nmid a$. Because of Fermat's Little Theorem,

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

□

Applications of Fermat's Theorem

1. We can verify a congruence.

   For example, let's find $5^{38} \equiv 4(\mod 11)$. Then:

$$5^{10} \equiv 1(\mod 11) \therefore (5^{10})^3 \equiv 1(\mod 11)$$

$$\therefore 5^{38} \equiv (5^{30})5^8 \equiv 5^8 \equiv (5^2)^4 \equiv 25^4 \equiv 3^4 \equiv 81 \equiv 4(\mod 81).$$

2. We can use the previous corollary to show that a divisor n is not prime when $a^n \not\equiv a(\mod n)$.

   For example, let's find if $n = 117$ is prime.

   Let $a = 2$. We will see if $2^n \equiv 2(\mod n)$ or not.

   We observe that

$$2^{117} = 2^{7\cdot16+5} = (2^7)^{16} 2^5 = 128^{16} 2^5.$$

   Then

$$\begin{aligned} 2^{117} &\equiv 128^{16} 2^5 \equiv 11^{16} 2^5 \equiv (11^2)^8 2^5 \\ &\equiv 121^8 2^5 \equiv 4^8 2^5 \equiv 2^{21} \\ &\equiv (2^7)^3 \equiv 128^3 \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44(\mod 117). \end{aligned}$$

   Because

$$2^{117} \equiv 44(\mod 117)$$

   and

$$2^{117} \not\equiv 2(\mod 117),$$

   it follows that 117 is a composite. Actually $117 = 9 \cdot 13$.

Lemma 1.3. *If p and q are distinct primes with $a^p \equiv a(\mod q)$ and $a^q \equiv a(\mod p)$ then $a^{pq} \equiv a(\mod pq)$.*

We should also note that the converse of Fermat's Little Theorem is not necessarily true.

For example, we can show that $2^{340} \equiv (\mod 341)$, but $341 = 11 \cdot 31$. The integers of the form $2^n - 2$ have received particular interest.

Definition 1.4. A composite integer n is called pseudoprime if $n \mid 2^n - 2$.

Theorem 1.5. *If n is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger pseudoprime.*

Proof. Proof strategy: First, show M_n is composite, then show $M_n \mid 2^{M_N} - 2$.

Let n be a pseudoprime. Then $n = rs$ for some $0 < r \leq s < n$. Then by Sec. 2.3, Prob. 21, $2^r - 1 \mid 2^n - 1 \therefore 2^r - 1 \mid M_n$.

Because r is not necessarily equal to n, M_n is composite. Then we have that

$$2^n \equiv s(\mod n) \therefore 2^n - 2 = kn,$$

for some $k \in \mathbb{Z}$.

Then $2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}$.

So $2^{M_n - 1} - 1 = 2^{kn} - 1 = (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \ldots + 2^n + 1)$.

Therefore $M_n \mid 2^{M_n - 1} - 1 \therefore M_n \mid 2^{M_n} - 2$, hence M_n is a pseudoprime. $\square$

Definition 1.6. A composite integer n for which $n \mid a^n - a$ is called a pseudoprime to the base a.

There are also integers that are pseudoprimes to every base a.

Definition 1.7. A composite integer n for which $a^{n-1} \equiv 1 (\mod n)$ to every base a with $\gcd(a, n) = 1$ is called an absolute pseudoprime.

We can show that that an absolute pseudoprime is square-free, i.e. it cannot be expressed as the square of an integer.

Theorem 1.8. *Let n be a composite square-free integer, $n = p_1 p_2 \dots p_r$ with r_i distinct primes. If $p_i - 1 \mid n - 1$ for $i = 1, 2, \dots, r$, then n is an absolute pseudoprime.*

Number Theory - MTSC 317
Lecture 13

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 10, 2014

1 The Sum and Number of Divisors

Any function whose domain is the set of positive integers is called a number-theoretic or arithmetic function.

Two popular and easy to handle number-theoretic functions are the functions τ and σ.

Definition 1.1. Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of the positive divisors of n.

For example, let $n = 12$. The positive divisors of 12 are 1, 2, 3, 4, 6, 12. Then

$$\tau(12) = 6$$

and

$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

We can show that $\tau(n) = 2$ iff n is a prime number, and $\sigma(n) = n + 1$ iff n is a prime number.

Related notations:
$\Sigma_{d|n} f(d)$: sum of $f(d)$ as d runs over the positive divisors of n.
For example: $\Sigma_{d|8} f(d) = f(1) + f(2) + f(4) + f(8)$.
Based on the previous notations we can write:

$$\tau(n) = \Sigma_{d|n} 1$$

$$\sigma(n) = \Sigma_{d|n} d.$$

Theorem 1.2. *If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form*

$$d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

where $0 \leq a_i \leq k_i (i = 1, 2, \dots, r)$.

Theorem 1.3. *If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then*

$$\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_r + 1)$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \dots \frac{p_1^{k_r+1} - 1}{p_r - 1}.$$

Proof. Strategy: Assume a positive divisor and its prime factorization. For $\tau(n)$, calculate all combinations of prime factors using the previous theorem. For $\sigma(n)$ multiply the binomial expansion of all prime factors to generate the sum of all divisors according to previous theorem. Then use algebraic identity to reach the product of fractions. □

Back to notation discussion, we usually denote products by Π.
Hence,

$$\Pi_{1 \leq d \leq 3} f(d) = f(1) \cdot f(2) \cdot f(3)$$

$$\Pi_{d|4} f(d) = f(1) \cdot f(2) \cdot f(4)$$

$$\Pi_{d|4, dprime} f(d) = f(1) \cdot f(2).$$

Example 1.1. Consider the number $180 = 2^2 \cdot 3^2 \cdot 5$. Then

$$\tau(180) = (2+1) \cdot (2+1) \cdot (1+1) = 18.$$

The divisors will have the form

$$2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}, \text{ with } a_1 = 0,1,2; a_2 = 0,1,2; a_1 = 0,1.$$

Also,

$$\begin{aligned}\sigma(180) &= \frac{2^{2+1}-1}{2-1} \cdot \frac{3^{2+1}-1}{3-1} \cdot \frac{5^{1+1}-1}{5-1} \\ &= \frac{7}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} \\ &= 7 \cdot 13 \cdot 6 \\ &= 546.\end{aligned}$$

A useful property of function τ is that the product of the positive divisors of an integer $n > 1$ is equal to $n^{\tau(n)/2}$, or equivalently

$$n^{\tau(n)/2} = \Pi_{d|n} d.$$

Definition 1.4. A number-theoretic function f is called multiplicative if

$$f(mn) = f(m) \cdot f(n).$$

whenever $gcd(m,n) = 1$.

Interesting notes

- The functions $f(n) = 1$ and $f(n) = n$ $\forall n \geq 1$ are multiplicative.
- We can use induction to show that

$$f(n_1 n_2 \ldots n_r) = f(n_1) f(n_2) \ldots f(n_r).$$

- Let $n \in \mathbb{Z}$. Given the canonical form $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and a multiplicative function f, it follows that

$$f(n) = f(p_1^{k_1}) f(p_2^{k_2}) \cdot f(p_r^{k_r}).$$

- Let f be a multiplicative function. Because $f(n) = f(n \cdot 1) = f(n) \cdot f(1)$, it follows that $f(1) = 1$ for any multiplicative function not identically zero.

Theorem 1.5. *The functions τ and σ are both multiplicative functions.*

Proof. Strategy: We assume two relatively prime integers m, n and their prime factorizations. Take their product, then use previous theorem to calculate $\tau(m \cdot n)$ and $\sigma(m \cdot n)$. Then show $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$ and $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$. □

Lemma 1.6. *If $gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, with $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$. Furthermore these products are all distinct.*

Theorem 1.7. *If f is a multiplicative function and F is defined by*

$$F(n) = \Sigma_{d|n} f(d)$$

then F is also multiplicative.

Proof. Strategy: We assume two relatively prime integers m, n and consider the set of positive divisors of $m \cdot n$ using the previous lemma. Let a multiplicative function f and show $F(mn) = F(m)F(n)$ using previous information. □

Example 1.2.

$$\begin{aligned}
F(8 \cdot 3) &= \Sigma_{d|24} f(d) \\
&= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24) \\
&= f(1 \cdot 1) + f(2 \cdot 1) + f(1 \cdot 3) + f(4 \cdot 1) + f(2 \cdot 3) + f(8 \cdot 1) + f(4 \cdot 3) + f(8 \cdot 3) \\
&= f(1) \cdot f(1) + f(2) \cdot f(1) + f(1) \cdot f(3) + f(4) \cdot f(1) + f(2) \cdot f(3) \\
&+ f(8) \cdot f(1) + f(4) \cdot f(3) + f(8) \cdot f(3) \\
&= [f(1) + f(2) + f(4) + f(8)][f(1) + f(3)] \\
&= \Sigma_{d|8} f(d) \cdot \Sigma_{d|3} f(d) \\
&= F(8)F(3).
\end{aligned}$$

Corollary 1.8. *The functions τ and σ are multiplicative.*

Number Theory - MTSC 317
Lecture 14

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 14, 2014

1 Eulers PHI-Function

Definition 1.1. For $n \geq 1$ let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

Example 1.1. Find $\phi(30)$.

We need to find the positive integers smaller than or equal to 30 that are relatively prime to 30.

These numbers are

$$1, 7, 11, 13, 17, 19, 23, 29.$$

Therefore, $\phi(30) = 8$.

We observe that the above list includes the prime numbers smaller than 30 except for the primes that factor 30, i.e., $30 = 2 \cdot 3 \cdot 5$, and their multiples.

Notes

- $\phi(1) = 1$, because $\gcd(1, 1) = 1$.
- For $n > 1$, $\gcd(n, n) = n \neq 1$, so $\phi(n)$ is equal to the number of relatively prime integers to n that are smaller than n.
- We can show that

  $$\phi(p) = p - 1 \text{ if and only if } p \text{ is prime.}$$

  If p is prime, then it is divisible by 1 and p only, therefore $\phi(p) = n-1$. If p is a composite number, then $\exists k \in \mathbb{Z}, k > 1 : k \mid p$. Therefore we have at least two integers k and n that divide n, hence $\phi(n) \leq n - 2$.

Theorem 1.2. *If p is a prime and $k > 0$ then*

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Proof. Strategy. Find integers between 1 and p^k divisible by p, then subtract this number from p^k to reach the result. $\square$

Lemma 1.3. *Given integers a, b, c,* $\gcd(a, bc) = 1$ *iff* $\gcd(a, b) = 1$ *and gcd$(a, c) = 1$.*

Theorem 1.4. *The function ϕ is a multiplicative function.*

Theorem 1.5. *If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then*

$$\begin{aligned}\phi(n) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

Proof. Proof strategy: utilize proof by induction, the previous lemma, and the fact that ϕ is a multiplicative function. □

Example 1.2. Find $\phi(360)$ using the previous theorem.

Prime factorization of 360 is $360 = 2^3 \cdot 3^2 \cdot 5$.

By the previous theorem it follows that

$$\begin{aligned}\phi(360) &= 360(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) \\ &= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \\ &= 360 \cdot \frac{4}{15} \\ &= 96.\end{aligned}$$

Theorem 1.6. *For $n > 2$, $\phi(n)$ is an even integer.*

Proof. Strategy. Use proof by cases to show that $\phi(n)$ is divisible by 2. Case 1: n is a power of 2. Case 2: n is not a power of 2, therefore is divisible by an odd prime. Use previous theorem, and the fact that $p - 1$ is divisible by 2 to complete the proof. □

Number Theory - MTSC 317
Lecture 15

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 19, 2014

1 Euler's Theorem

Lemma 1.1. *Let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then*

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Theorem 1.2 (Euler)**.** *If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 (\mod n)$.*

Proof. Strategy: take all positive integers less than n that are relatively prime to n. We use previous lemma to produce the set of congruences and multiply the congruences. Then use lemma of previous section to reach the final result. □

Corollary 1.3 (Fermat). *If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$.*

Example 1.1. Find the last two digits in the decimal representation of 3^{256}.

This question is equivalent to that of finding the smallest nonnegative integer to which 3^{256} is congruent modulo 100.

Because $\gcd(3, 100) = 1$ and

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5}) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40,$$

by Euler's theorem it follows that

$$3^{\phi(100)} \equiv 1 \pmod{100} \therefore 3^{40} \equiv 1 \pmod{100}.$$

By the Division Algorithm $256 = 6 \cdot 40 + 16$, so

$$3^{256} = 3^{6 \cdot 40 + 16} = (3^{40})^6 \cdot 3^{16} \equiv 3^{16} \pmod{100}.$$

Then

$$\begin{aligned} 3^2 &\equiv 9 \pmod{100} \\ 3^4 &\equiv 9^2 \equiv 81 \pmod{100} \\ 3^8 &\equiv 81^2 \equiv (-19)^2 \equiv 361 \equiv 61 \pmod{100} \\ 3^{16} &\equiv 61^2 \equiv (-39)^2 \equiv 1521 \equiv 21 \pmod{100}. \end{aligned}$$

Applications of Euler's theorem

- Different proof of the Chinese Remainder Theorem.
- If n is an odd integer that is not a multiple of 5, then n divides an integer all of whose digits are equal to 1. One example is $7 \mid 111111$.

Number Theory - MTSC 317
Lecture 16

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 21, 2014

1 Order of an Integer Modulo n

Definition 1.1. Let $n > 1$ and $\gcd(a, n) = 1$. The order of a modulo n, or the exponent to which a belongs modulo n, is the smallest integer k such that $a^k \equiv 1 (\mod n)$.

Let us find the order of 2 modulo 7. By inspection we have that

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1, \ldots$$

Observe that the integer 2 has order 3 modulo 7.

Theorem 1.2. *Let the integer a have order k modulo n. Then $a^h \equiv 1 (\mod n)$ if and only if $k \mid h$; in particular $k \mid \phi(n)$.*

We can use the previous theorem to narrow down our search for the order of integer a modulo n by considering powers that are divisors of $\phi(n)$.

For example, let us find the order of 2 modulo 13. Because $\phi(13) = 12$ our search ranges over the divisors of 12 that us 1, 2, 3, 4, 6, 12:

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^6 \equiv 12, 2^{12} \equiv 1 (\mod 13).$$

Therefore 2 has order 12 modulo 13.

Theorem 1.3. *If the integer a has order k modulo n, then $a^i \equiv a^j \pmod{n}$ if and only if $i \equiv j \pmod{k}$.*

Corollary 1.4. *If a has order k modulo n, then the integers $a, a^2, \ldots, a^k$ are incongruent modulo n.*

Theorem 1.5. *If the integer a has order k modulo n and $h > 0$, then a^h has order $k/\gcd(h,k)$ modulo n.*

Corollary 1.6. *Let a have order k modulo n. Then a^h also has order k if and only if $\gcd(h,k) = 1$.*

Definition 1.7. If $\gcd(a,n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a primitive root of the integer n.

Note that 3 is a primitive root of 7 because

$$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^6 \equiv 1 \pmod{7}.$$

Example 1.1. We can show that if $F_n = 2^{2^n} + 1, n > 1$ is a prime, then 2 is not a primitive root of F_n.

Observe that $2^{2^{n+1}} - 1 = (2^{2^n} - 1) \cdot (2^{2^n} + 1)$, so $2^{2^{n+1}} \equiv 1 \pmod{F_n}$.

By definition the order of 2 modulo F_n is smaller than or equal to 2^{n+1}. Because F_n is prime,

$$\phi(F_n) = F_n - 1 = 2^{2^n}.$$

Also, we can show that $2^{2^n} > 2^{n+1}$, when $n > 1$.

Hence the order of 2 modulo F_n is smaller than $\phi(F_n)$. Therefore 2 can not be a primitive root of F_n.

Theorem 1.8. *Let* $\gcd(a, n) = 1$ *and let* $a_1, a_2, \ldots, a_{\phi(n)}$ *be the positive integers less than* n *and relatively prime to* n*. If* a *is a primitive root of* n*, then*

$$a^1, a^2, \ldots, a^{\phi(n)}$$

are congruent modulo n *to* $a_1, a_2, \ldots, a_{\phi(n)}$*, in some order.*

Corollary 1.9. *If* n *has a primitive root, then it has exactly* $\phi(\phi(n))$ *of them.*

Number Theory - MTSC 317
Lecture 17

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 9, 2014

1 Primitive Roots for Primes

Theorem 1.1 (Lagrange). *If p is a prime and*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence

$$f(x) \equiv (\mod p)$$

has at most n incongruent solutions modulo p.

Corollary 1.2. *If p is a prime number and $d \mid p-1$, then the congruence*

$$x^d - 1 \equiv 0(\mod p)$$

has exactly d solutions.

Theorem 1.3. *If p is a prime number and $d \mid p-1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p.*

Corollary 1.4. *If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots of p.*

Example 1.1.

Number Theory - MTSC 317
Lecture 18

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 9, 2014

1 Euler's Criterion

The Quadratic Reciprocity Law deals with the solvability of quadratic congruences.

Definition 1.1. Let p be an odd prime and $\gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a(\mod p)$ has a solution, then a is a quadratic residue of p. Otherwise, a is called a quadratic nonresidue of p.

Theorem 1.2 (Euler's criterion)**.** *Let p be an odd prime and* $\gcd(a, p) = 1$. *Then a is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1(\mod p)$.*

Corollary 1.3. *Let p be an odd prime and* $\gcd(a, p) = 1$. *Then a is a quadratic residue or nonresidue of p according to whether*

$$a^{(p-1)/2} \equiv 1(\mod p)$$

or

$$a^{(p-1)/2} \equiv -1(\mod p).$$

Example 1.1.

Number Theory - MTSC 317
Lecture 19

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 9, 2014

1 The Legendre Symbol and its Properties

Definition 1.1. Let p be an odd prime and let $\gcd(a, p) = 1$. The Legendre symbol (a/p) is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

For the want of better terminology, we shall refer to a as the numerator and p as the denominator of the symbol (a/p). Another standard notation for the Legendre symbol is $(\frac{a}{p})$, or $(a \mid p)$.

Example 1.1.

Theorem 1.2. *Let p be an odd prime and let a and b be integers that are relatively prime to p. Then the Legendre symbol has the following properties:*

1. *If $a \equiv b (\mod p)$, then $(a/p) = (b/p)$*
2. $(a^2/p) = 1$
3. $(a/p) \equiv a^{(p-1)/2} (\mod p)$
4. $(ab/p) = (a/p)(b/p)$

5. $(1/p) = 1$ *and* $(-1/p) = (-1)^{(p-1)/2}$.

Corollary 1.3. *If p is an odd prime, then*

$$(-1/p) = \begin{cases} 1 & mboxifp \equiv 1 (\mod 4) \\ -1 & mboxifp \equiv 3 (\mod 4) \end{cases}.$$

Example 1.2.

Theorem 1.4. *There are infinitely many primes of the form $4k+1$.*

Theorem 1.5. *If p is an odd prime, then*

$$\Sigma_{a=1}^{p-1}(a/p) = 0.$$

Therefore, there are precisely $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues of p.

Corollary 1.6. *The quadratic residues of an odd prime p are congruent modulo p to the even powers of a primitive root r of p; the quadratic non residues are congruent to the odd powers of r.*

Theorem 1.7 (Gauss's lemma)**.** *Let p be an odd prime and let $\gcd(a,p) = 1$. If n denotes the number of integers in the set*

$$S = \left\{ a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a \right\}$$

whose remainders upon division by p exceed $p/2$, then

$$(a/p) = (-1)^n.$$

Theorem 1.8. *If p is an odd prime, than*

$$(2/p) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 8 \textit{ or } p \equiv 7 \pmod 8 \\ -1 & \textit{if } p \equiv 3 \pmod 8 \textit{ or } p \equiv 5 \pmod 8 \end{cases}$$

Corollary 1.9. *If p is an odd prime, then*

$$(2/p) = (-1)^{(p^2-1)/8}.$$

Theorem 1.10. *If p and $2p+1$ are both odd primes, then the integer $(-1)^{(p-1)/2}2$ is a primitive root of $2p+1$.*

Theorem 1.11. *There are infinitely many primes of the form $8k-1$.*

Lemma 1.12. *If p is an odd prime and a an odd integer with $\gcd(a,p)=1$, then*

$$(a/p) = (-1)\Sigma_{k=1}^{(p-1)/2}[ka/p].$$

Number Theory - MTSC 317
Lecture 20

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 9, 2014

1 Quadratic Reciprocity

Theorem 1.1. *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Corollary 1.2. *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Corollary 1.3. *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = \begin{cases} (q/p) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -(q/p) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Example 1.1.

Theorem 1.4. *If* $p \neq 3$ *is an odd prime, then*

$$(3/q)(q/p) = \begin{cases} 1 & \textit{if } p \equiv \pm 1 \pmod{12} \\ -1 & \textit{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Example 1.2.