Elementary Number Theory

MARUCO

Summer, 2018
Problem Set #0

Terminology

axiom, theorem, proof, $\mathbb{Z}$, $\mathbb{N}$.

Axioms

Make a list of axioms for the integers. Does your list adequately describe them? Can you make this list as short as possible? To help you construct your list, here are a few facts that we know to be true about the integers that you would want to be able to prove from your axioms:

- If $a \cdot b = 0$ then $a = 0$ or $b = 0$.
- If $a^2 = 1$ then $a = \pm 1$.
- There are no integers between 0 and 1.
**Problem Set #1.1**

**The Division Algorithm:** Given integers $a$ and $b$, with $b > 0$, there exist unique integers $q$ and $r$ satisfying
\[ a = qb + r \quad 0 \leq r < b. \]

The integers $q$ and $r$ are called respectively, the *quotient* and *remainder*.

**Terminology**

divides, greatest common divisor, relatively prime

**Conjectures**

(prove, disprove, or salvage if possible)

1.1 Let $a, b$ and $c$ be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

1.2 Let $a, b$ and $c$ be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.

1.3 Let $a, b$ and $c$ be integers. If $a \mid b$ and $a \mid c$, then $a \mid bc$.

1.4 Let $a, n, b, r$ be integers. If $a = nb + r$ and $k \mid a$ and $k \mid b$ then $k \mid r$.

1.5 Let $a, b, n_1$ and $r_1$ be integers with $a$ and $b$ not both 0. If $a = n_1b + r_1$, then $\gcd(a, b) = (b, r_1)$. 
Problem Set #1.2

Exercises

1. Once you’ve established conjecture 1.5, you can use it to develop a general procedure for finding the gcd of two integers. (Since you developed it, this is really your algorithm, but the first guy to do it was Euclid, so we usually call it the Euclidean algorithm.)

2. Use your algorithm to find gcd(175, 24), gcd(10, 256), gcd(112, –96).

3. Find integers x and y such that 175x + 24y = 1. After establishing conjecture 1.13, find all integers x and y which are solutions to 175x + 24y = 1.

Conjectures

1.6 Let a and b be integers. If gcd(a, b) = 1, then there exist integers x and y such that \( ax + by = 1 \).

1.7 Let a and b be integers. If there exist integers x and y with \( ax + by = 1 \), then gcd(a, b) = 1.

1.8 Let a and b be integers. Then gcd(a, b) = 1, if and only if there exist integers x and y such that \( ax + by = 1 \).

1.9 Let a and b be integers. Then there exist integers x and y such that \( ax + by = \gcd(a, b) \).

1.10 Let a and b be integers. Then \( \gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1 \).

1.11 Let a, b and c be integers. If a \mid bc and gcd(a, b) = 1, then a \mid c.

1.12 Given integers a, b and c, there exist integers x and y that satisfy the equation \( ax + by = c \) if and only if \( \frac{b}{\gcd(a,b)} \).

1.13 If \( x_0 \) and \( y_0 \) are solutions to the linear diophantine equation \( ax + by = c \), then all other solutions are given by

\[
x = x_0 + \frac{b}{\gcd(a,b)} t \quad \text{and} \quad y = y_0 - \frac{a}{\gcd(a,b)} t
\]

where \( t \) is an arbitrary integer. (Hint: This proof is really two parts. First you need to show that the above equations actually give a solution. Then you need to show that any solution is actually of the form above.)
Problem Set #2.1

The Fundamental Theorem of Arithmetic Every natural number greater than 1 is either a prime number, or it can be expressed as a finite product of prime numbers where the expression is unique up to the order of the factors.

Terminology

prime, composite, prime factorization

Exercises

1. Without using a calculator, write down all of the primes from 1-100. How did you know they were primes?

2. Find gcd(3^{14} \cdot 7^{22} \cdot 11^{5} \cdot 17^{3}, 5^{2} \cdot 11^{4} \cdot 13^{8} \cdot 17). Is there a better method here than the division algorithm? Why is it better? Is it always better?

Conjectures

2.1 If p is a prime number and p | ab, then p | a or p | b.

2.2 If p is a prime number and p | a_1 \cdots a_k, then p | a_i for some 1 \leq i \leq k.

2.3 If p, q_1, ..., q_k are prime numbers and p | q_1 \cdots q_k then p = q_i for some 1 \leq i \leq k.

2.4 A natural number n is prime if and only if for all primes p \leq \sqrt{n}, p does not divide n.

2.5 Let a and b be natural numbers greater than 1 and let p_1^{r_1}p_2^{r_2} \cdots p_m^{r_m} be the unique prime factorization of a and let q_1^{t_1}q_2^{t_2} \cdots q_s^{t_s} be the unique prime factorization of b. Then a | b if and only if for all i \leq m there exists a j \leq s such that p_i = q_j and r_i \leq t_j.

2.6 If a, b and n are natural numbers and a^n | b^n, then a | b.
Problem Set #2.2

Dirichlet’s Theorem of Primes in an Arithmetic Progression If $a$ and $b$ are relatively prime natural numbers, then the arithmetic progression

$$a, a+b, a+2b, a+3b, \ldots$$

contains infinitely many prime numbers. In other words, there are infinitely many primes of the form $bk + a$.

Terminology

arithmetic progression, factorial

Conjectures

2.7 Let $a, b$ and $c$ be integers. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

2.8 Let $a, b, u$ and $v$ be integers. If $\gcd(a, b) = 1$ and $u \mid a$ and $v \mid b$, then $\gcd(u, v) = 1$.

2.9 Let $a$ and $b$ be integers If $a \mid b$, then $a \nmid b + 1$.

2.10 Let $k$ be a natural number. Then there exists a natural number $n$ which is not divisible by any number between $k$ and 1.

2.11 Let $k$ be a natural number. Then there exists a prime larger than $k$.

2.12 There are infinitely many prime numbers.
Problem Set #3.1

Terminology
congruence modulo m

Exercises
1. Using theorems 3.1-3.6, show that 41 divides $2^{20} - 1$.

Conjectures
3.1 $a \equiv a \mod n$ for any integer $a$.
3.2 If $a \equiv b \mod n$, then $b \equiv a \mod n$.
3.3 If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.
3.4 If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.
3.5 If $a \equiv b \mod n$, then $a + c \equiv b + c \mod n$ and $ac \equiv bc \mod n$.
3.6 If $a \equiv b \mod n$, then $a^k \equiv b^k \mod n$ for any positive integer $k$.
3.7 Given any integer $a$ and any natural number $n$, there exists a unique integer $t$ in the set \{0, 1, 2, ..., $n - 1$\} such that $a \equiv t \mod n$. 
The Chinese Remainder Theorem: Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$
\begin{align*}
    x &\equiv a_1 \mod n_1 \\
    x &\equiv a_2 \mod n_2 \\
    &\vdots \\
    x &\equiv a_r \mod n_r \\
\end{align*}
$$

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

**Terminology**

residue system, canonical residue system

**Exercises**

1. Find all solutions in the appropriate canonical residue system for $26x \equiv 14 \mod 3$ and $4x \equiv 7 \mod 8$. How did you do that?

**Conjectures**

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

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

3.10 Let $a, b$ and $n$ be integers with $n > 0$. Show that $ax \equiv b \mod n$ has a solution if and only if there exist integers $x$ and $y$ such that $ax + ny = b$.

3.11 Let $a, b$ and $n$ be integers with $n > 0$. The equation $ax \equiv b \mod n$ has a solution if and only if $\gcd(a, n) | b$.

3.12 Let $a, b$ and $n$ be integers with $n > 0$. Suppose that $x_0$ is a solution to the congruence $ax \equiv b \mod n$, then all solutions are given by $x_0 + \frac{n}{\gcd(a, n)} \cdot t$ where $t \in \mathbb{Z}$.

3.13 Let $a, b$ and $n$ be integers with $n > 0$, let $d = \gcd(a, n)$. If the congruence $ax \equiv b \mod n$ has a solution $x_0$, then it has precisely $d$ mutually incongruent solutions modulo $n$, given by $x_0 + \frac{n}{\gcd(a, n)} \cdot t$ where $t \in \{0, \ldots, d - 1\}$.
Problem Set #4.1

Terminology

order of $a$ modulo $n$

Exercises

1. Compute $\text{ord}_3(5)$ and $\text{ord}_5(2)$. What happens if you try to compute $\text{ord}_4(2)$?

2. After proving the conjectures on this page, can you say anything about the size of $\text{ord}_n(a)$ relative to $n$?

Conjectures

4.1 Let $a$ and $n$ be natural numbers with $\gcd(a, n) = 1$, then $\gcd(a^j, n) = 1$ for any natural number $j$.

4.2 Let $a, b$ and $n$ be integers, $n > 0$ and $\gcd(a, n) = 1$. If $a \equiv b \mod n$ then $\gcd(b, n) = 1$.

4.3 Let $a$ and $n$ be natural numbers. Then there exist natural numbers $i$ and $j$ with $i \neq j$ such that $a^i \equiv a^j \mod n$.

4.4 Let $a$ and $n$ be natural numbers with $\gcd(a, n) = 1$. Then there exists a natural number $k$ such that $a^k \equiv 1 \mod n$.

4.5 Let $a$ and $n$ be natural numbers with $\gcd(a, n) = 1$ and let $k = \text{ord}_n(a)$. Then the numbers $a^1, a^2, ..., a^k$ are pairwise incongruent modulo $n$.

4.6 Let $a$ and $n$ be natural numbers with $\gcd(a, n) = 1$ and let $k = \text{ord}_n(a)$. For any natural number $m$, $a^m$ is congruent modulo $n$ to one of the numbers $a^1, a^2, ..., a^k$.

4.7 Let $a$ and $n$ be natural numbers with $\gcd(a, n) = 1$ and let $m$ be a natural number. Then, $a^m \equiv 1 \mod n$ if and only if $\text{ord}_n(a) | m$.

4.8 Let $p$ be a prime. If $a$ is an integer and $p$ does not divide $a$ then $\{a, 2a, ..., pa\}$ is a residue system modulo $p$.

4.9 Let $p$ be a prime and let $a$ be an integer not divisible by $p$. Then

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \mod p.$$ 

4.10 (Fermat's Little Theorem) If $p$ is a prime, then $a^p \equiv a \mod p$ for any integer $a$. 
Problem Set #4.2

Terminology

$\mathbb{Z}_n$, $\mathbb{Z}_n^\times$, Euler $\phi$-function, inverse modulo $n$

Exercises

1. Compute the inverses of 2, 3, and 4 modulo 7.

2. Can you say anything about the size of $\mathbb{Z}_n^\times$? What about $\mathbb{Z}_p^\times$ for $p$ primes?

3. After proving the conjectures on this page (especially 4.12), what is the relationship between $\mathbb{Z}_n^\times$ and inverses? Can you improve your definition of $\mathbb{Z}_n^\times$?

Conjectures

4.11 If $p$ and $q$ are distinct primes with $a^p \equiv a \mod q$ and $a^q \equiv a \mod p$ then $a^{pq} \equiv a \mod pq$.

4.12 Suppose that $\gcd(a,n) = 1$. Then there exists a unique $b \in \mathbb{Z}_n^\times$, such that $a \cdot b \equiv 1 \mod n$.

4.13 If $p$ is a prime, then every non-zero element in $\mathbb{Z}_p$ has an inverse in $\mathbb{Z}_p$.

4.14 If $p$ is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p - 2) \equiv 1 \mod p$.

4.15 (Wilson's Theorem) If $p$ is prime, then $(p - 1)! \equiv -1 \mod p$.

4.16 Suppose that $x_i, x_j \in \mathbb{Z}_n^\times$ and $\gcd(a,n) = 1$. If $ax_i \equiv ax_j \mod n$, then $x_i = x_j$.

4.17 Suppose that $x_i \in \mathbb{Z}_n^\times$ and $\gcd(a,n) = 1$. There exists $x_j \in \mathbb{Z}_n^\times$ such that $ax_i \equiv x_j \mod n$.

4.18 If $\gcd(a,n) = 1$ and $\mathbb{Z}_n^\times = \{x_1, \ldots, x_{\phi(n)}\}$, then

$$ax_1 \cdot ax_2 \cdot \ldots \cdot ax_{\phi(n)} \equiv x_1 \cdot x_2 \cdot \ldots \cdot x_{\phi(n)} \mod n.$$

4.19 (Euler’s Theorem) If $a$ and $n$ are integers, $n > 0$ and $\gcd(a,n) = 1$, then

$$a^{\phi(n)} \equiv 1 \mod n.$$
Problem Set #5.1

The classical caesar cipher replaces letters with their alphanumerical values modulo \( n \) to encode a message. So with this fixed alphanumeric system:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

1. A letter \( x \) is encoded by replacing it with the letter corresponding to \( x + n \mod 26 \).
2. A letter \( x \) is decoded by replacing it with the letter corresponding to \( x - n \mod 26 \).
3. Without knowing what \( n \) is, use frequency analysis to decode the following message:

POBWKD SC K VSKB

Conjectures

In what following, we may need to assume (without proof) that the Euler \( \phi \)-function is multiplicative, that is, for integers relatively prime integers \( a \) and \( b \), \( \phi(ab) = \phi(a) \cdot \phi(b) \).

5.1 Suppose that \( E \) is a natural number with \( (E, \phi(pq)) = 1 \). Then there exists a natural number \( D \) such that \( DE \equiv 1 \mod \phi(pq) \).

5.2 Suppose that \( p \) and \( q \) are distinct prime numbers with \( 0 \leq m < pq \), and suppose that \( D \) and \( E \) are natural numbers satisfying \( DE \equiv 1 \mod \phi(pq) \). If \( m^E \equiv c \mod (pq) \) then \( c^D \equiv m \mod (pq) \).

RSA Key Generation

1. Choose distinct primes \( p \) and \( q \), both larger than 26.
2. Compute \( n = pq \).
3. Compute \( \phi(n) = \phi(pq) = \phi(p) \cdot \phi(q) = (p - 1) \cdot (q - 1) \)
4. Choose an integer \( E \) where \( (E, \phi(n)) = 1 \). Now \( (n, E) \) is your public key.
5. Compute \( D \), so that \( ED \equiv 1 \mod \phi(n) \). Now \( (n, D) \) is your private key.
RSA Encryption/Decryption

1. Give your public key to a partner, keep your private key to yourself.

2. Convert a message $M$ into a string of integers $m_1, m_2, ..., m_k$ using the alphanumeric table above.

3. For each integer $m_i$ in the string, compute $c_i \equiv m_i^e \mod n$ and send the string $c_1, c_2, ..., c_k$ to your partner.

4. To decode the message, your partner just needs to solve $m_i \equiv c_i^d \mod n$, and convert the $m_i$ back into letters.
Problem Set #5.2

The polyalphabetic Caesar cipher is a more sophisticated version of the classical cipher. Starting with the same alphanumeric system:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

1. A secret codeword is chose, let’s say: GAUSS

2. A message is encoded by performing the following addition, term by term, modulo 26:

<table>
<thead>
<tr>
<th>F</th>
<th>E</th>
<th>R</th>
<th>M</th>
<th>A</th>
<th>T</th>
<th>I</th>
<th>S</th>
<th>A</th>
<th>L</th>
<th>I</th>
<th>A</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>A</td>
<td>U</td>
<td>S</td>
<td>S</td>
<td>G</td>
<td>A</td>
<td>U</td>
<td>S</td>
<td>S</td>
<td>G</td>
<td>A</td>
<td>U</td>
</tr>
</tbody>
</table>

3. Using codeword GAUSS, decode the following message:

CIHLWX IM UGSIHY

Terminology

primitive root modulo $p$

Conjectures

For the following proofs we will assume that primitive roots exists for every prime $p$, although we won’t actually prove that until problem set 6.

5.3 Let $p$ be prime, then $g$ is a primitive root modulo $p$ if and only if for every divisor $n \neq 1$ of $p - 1$, we have $g^{p-1} \equiv 1 \mod p$.

5.4 Let $p$ be a prime. Then $g$ is a primitive root modulo $p$ if and only if \{0, $g, g^2, \ldots, g^{p-1}\}$ forms a residue system modulo $p$. 
Diffie Helman Key Generation

This protocol allows partners, call them Alice and Bob, to communicate.

1. Alice and Bob agree on a big prime number $p$ and a primitive root $g$.

2. Alice chooses a secret number, $S_A$, and Bob chooses one, $S_B$.

3. Alice and Bob compute $P_A \equiv g^{S_A} \mod p$ and $P_B \equiv g^{S_B} \mod p$, these are their public keys.

4. Now Alice and Bob can compute their shared key, $k \equiv g^{S_A S_B} \mod p$, which Alice gets by computing
   
   $$P_B^{S_A} \equiv g^{S_A S_B} \mod p$$

   and Bob gets by computing
   
   $$P_A^{S_B} \equiv g^{S_A S_B} \mod p.$$  

Diffie Helman Encryption/Decryption

1. With a partner agree on a prime $p > 26$ and find a primitive root $g$.

2. Choose your private key (don’t share this with anybody, even your partner).

3. After doing the necessary computations, swap public keys and compute your encryption key, $k$.

4. Convert a message $M$ into a string of integers $m_1, m_2, ..., m_n$ using the alphanumeric table above.

5. Encode your message by replacing $m_i$ with $c_i$ where
   
   $$c_i \equiv k \cdot m_i \mod p.$$  

   and send your partner the string $c_1, c_2, ..., c_n$.

6. Decode your message by solving $c_i \equiv k \cdot m_i \mod p$ for $m_i$ for every $i$. 

Problem Set #6.1

Terminology

primitive root modulo \( n \).

Exercises

1. Do 3, 4, and 5 have primitive roots? How about 8?

Conjectures

6.1 If \( a \) is a primitive root modulo \( n \), then \( \{ a, a^2, \ldots, a^{\phi(n)} \} \) forms a reduced residue system modulo \( n \).

6.2 If \( p \) is prime and \( a \) is a primitive root modulo \( p \), then \( \{ 0, a, \ldots, a^{p-1} \} \) forms a residue system modulo \( p \).

6.3 Let \( f(x) \) be a polynomial of degree \( n \). Then \( r \) is a root of \( f(x) \) if and only if

\[
f(x) = (x - r) \cdot g(x)
\]

where \( g(x) \) is a polynomial of degree \( n - 1 \).

6.4 Let \( f(x) \) be a polynomial of degree \( n \), let \( p \) be a prime, and let \( r \) be an integer. Then

\[
f(r) \equiv 0 \mod p
\]

if and only if

\[
f(x) \equiv (x - r) \cdot g(x) \mod p
\]

where \( g(x) \) is a polynomial of degree \( n - 1 \).

6.5 (Lagrange’s Theorem) Let \( f(x) \) be a polynomial of degree \( n \), and let \( p \) be a prime. Then

\[
f(x) \equiv 0 \mod p
\]

has at most \( n \) incongruent solutions.

6.6 Let \( p \) be prime. For any \( d \mid p - 1 \), the congruence \( x^d - 1 \equiv 0 \mod p \) has exactly \( d \) incongruent solutions.
Exercises

1. Compute $\sum_{d|8} \phi(d)$ and $\sum_{d|12} \phi(d)$, and then make a conjecture.

Conjectures

6.7 Let $p$ be prime, then $\sum_{d|p} \phi(d) = p$.

6.8 Let $p$ be prime and $k$ a positive integer, then $\sum_{d|p^k} \phi(d) = p^k$.

6.9 If $p$ and $q$ are two different primes, then $\sum_{d|pq} \phi(d) = pq$.

6.10 If $m$ and $n$ are two relatively prime positive integers, then

$$\left( \sum_{d|m} \phi(d) \right) \cdot \left( \sum_{d|n} \phi(d) \right) = \sum_{d|mn} \phi(d).$$

6.11 For any natural number $n$, we have $\sum_{d|n} \phi(d) = n$

6.12 Let $p$ be a prime, and let $a$ be an integer relatively prime to $p$ with ord$_p(a) = d$. Then ord$_p(a^k) = d$ if and only if gcd$(d, k) = 1$.

6.13 Let $p$ be prime. Then for any $a \in \mathbb{Z}_p^\times$, we have ord$_p(a) \mid p-1$.

6.14 Let $p$ be prime. For any $d \mid p-1$, there are exactly $\phi(d)$ many incongruent integers having order $d$ modulo $p$.

6.15 For $p$ prime, there are exactly $\phi(p-1)$ incongruent primitive roots modulo $p$.

6.16 (Primitive Root Test) Let $p$ be a prime. Then $a$ is a primitive root modulo $p$, if and only if for all factors $f$ of $p-1$ other than 1,

$$a^{\frac{p-1}{f}} \not\equiv 1 \mod p.$$
Problem Set #6.3

Conjectures

6.17 If $a$ is an integer and $\nu$ and $n$ are natural numbers such that $\gcd(a, n) = 1$, then

$$a^{\nu \phi(n) + 1} \equiv a \mod n.$$  

6.18 If $k, n$ are natural numbers with $\gcd(k, \phi(n)) = 1$, then there exist positive integers $u$ and $\nu$ satisfying

$$ku = \nu \phi(n) + 1.$$  

6.19 If $b$ is an integer and $k$ and $n$ are natural numbers such that $(k, \phi(n)) = 1$ and $(b, n) = 1$, then $x^k \equiv b \mod n$ has a unique solution modulo $n$. Moreover, that solution is given by

$$x \equiv b^u \mod n$$

where $u$ and $v$ are positive integers such that $ku = \phi(n)v + 1$.  

Problem Set #7.1

Terminology
quadratic residue

Conjectures

7.1 Suppose $a$ is an integer and $p$ is an odd prime with $(a,p) = 1$. Then finding a solution, $x$, to the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

is equivalent to solving $y^2 \equiv b^2 - 4ac \pmod{p}$ for $y$ and then solving $2ax \equiv y - b \pmod{p}$ for $x$.

7.2 Let $p$ be an odd prime. Then half the numbers not congruent to 0 in any complete residue system modulo $p$ are perfect squares modulo $p$ and half are not.

7.3 Let $p$ be an odd prime. Then half the numbers not congruent to 0 in any complete residue system modulo $p$ are quadratic residues modulo $p$ and half are quadratic nonresidues modulo $p$.

7.4 Suppose $p$ is an odd prime and $p$ does not divide either of the two integers $a$ or $b$. Then,

(a) if $a$ and $b$ are both quadratic residues modulo $p$, then $ab$ is a quadratic residue modulo $p$.

(b) if $a$ is a quadratic residue modulo $p$, and $b$ is a quadratic nonresidue modulo $p$, then $ab$ is a quadratic nonresidue modulo $p$.

(c) if $a$ and $b$ are both quadratic nonresidues modulo $p$, then $ab$ is a quadratic residue modulo $p$.

7.5 Suppose $p$ is an odd prime and $p$ does not divide either $a$ or $b$. Then,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

7.6 Suppose $p$ is an odd prime and $p$ does not divide the natural number $a$. Then, $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. 
Conjectures

7.7 (Euler’s Criterion) Suppose \( p \) is an odd prime and \( p \) does not divide the natural number \( a \). Then \( a \) is a quadratic residue modulo \( p \) if and only if \( a^{\frac{p-1}{2}} \equiv 1 \mod p \); and \( a \) is a quadratic nonresidue modulo \( p \) if and only if \( a^{\frac{p-1}{2}} \equiv -1 \mod p \). The criterion can be abbreviated using the Legendre symbol:

\[
a^{\frac{p-1}{2}} \equiv \left( \frac{a}{p} \right) \mod p.
\]

7.8 Let \( p \) be an odd prime. Then \(-1\) is a quadratic residue modulo \( p \) if and only if \( p \) is of the form \( 4k + 1 \) for some integer \( k \). Or, equivalently,

\[
\left( \frac{-1}{p} \right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv 3 \mod 4. \end{cases}
\]

7.9 Let \( p \) be a prime, \( a \) an integer not divisible by \( p \) and \( r_1, r_2, \ldots, r_{\frac{p-1}{2}} \) the representatives of \( a, 2a, \ldots, \frac{p-1}{2}a \) in the complete residue system

\[
\left\{ -\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2} \right\}.
\]

Then

\[ r_1 \cdot r_2 \cdot \ldots \cdot r_{\frac{p-1}{2}} = (-1)^g \frac{p-1}{2}! \]

where \( g \) is the number of \( r_i \)'s which are negative.

7.10 (Gauss’ Lemma) Let \( p \) be a prime and \( a \) an integer not divisible by \( p \). Let \( g \) be the number of negative representatives of \( a, 2a, \ldots, \frac{p-1}{2}a \) in the complete residue system \( \left\{ -\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2} \right\} \). Then,

\[
\left( \frac{a}{p} \right) = (-1)^g
\]

7.11 Let \( p \) be an odd prime, then

\[
\left( \frac{2}{p} \right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \mod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \mod 8. \end{cases}
\]

7.12 (Quadratic Reciprocity) Let \( p \) and \( q \) be odd primes, then

\[
\left( \frac{p}{q} \right) = \begin{cases} \left( \frac{q}{p} \right) & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\ -\left( \frac{q}{p} \right) & \text{if } p \equiv q \equiv 3 \mod 4. \end{cases}
\]