Math 620: Homework 2, Congruence

Due on Friday, September 11, 2015

Boynton 10:00

Kailee Gray

Exercise 1

Exercise 1.3.4 from B&B: Solve the conguence $20x \equiv 12 \pmod{72}$.

Note $\gcd(20, 72) = 4$. Note $4 \mid 12$ so there will be 4 distinct solutions modulo 72. If $20x \equiv 12 \pmod{72}$, $20x = 12 + 72k$ for some integer k. 20, 12, 72 are all divisible by 4, so the previous equation is equivalent to $5x = 3 + 18k$. This yields the congruence

$$5x \equiv 3 \pmod{18}. \tag{1}$$

Since $\gcd(5, 18) = 1$ proposition 1.3.4 in B&B implies there exists some integer b such that $5b \equiv 1$(mod 18. Apply the extended Euclidean Algorithm to find this b:

$$18 = 3 \cdot 5 + 3 \Leftrightarrow 3 = 18 - 3 \cdot 5, \qquad 5 = 3 \cdot 1 + 2 \Leftrightarrow 2 = 5 - 3 \cdot 1, \qquad 3 = 2 \cdot 1 + 1 \Leftrightarrow 1 = 3 - 2 \cdot 1.$$

Then, using back substitution we have

$$1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 2 \cdot 3 - 5 = 2 \cdot (18 - 3 \cdot 5) - 5 = 2 \cdot 18 - 6 \cdot 5 - 5 = 2 \cdot 18 - 7 \cdot 5$$

. Thus, $b = -7$ which is equivalent to 11 mod 18. So, multiply both sides of equation (1) by 11 to obtain

$$11 \cdot 5x \equiv 11 \cdot 3 \pmod{18} \Leftrightarrow 55x \equiv 33 \pmod{18} \Leftrightarrow 1 \cdot x \equiv 15 \pmod{18} \Leftrightarrow x \equiv 15 \pmod{18}$$

Hence, the solutions of the given congruence are $15,\ 33,\ 51,\ 69$ mod 72.

Exercise 2

Exercise 1.3.12 of B&B: Show that $4 \cdot (n^2 + 1)$ is never divisible by 11.

Proof. If there was an integer n such that $11 \mid 4 \cdot (n^2 + 1)$, then $4 \cdot (n^2 + 1) \equiv 0 \pmod{11}$. Suppose there is such an n. If $4 \cdot (n^2 + 1) \equiv 0 \pmod{11}$, then $4n^2 + 4 \equiv 0 \pmod{11}$ and $4n^2 \equiv -4 \pmod{11}$. Because $gcd(4, 11) = 1$, $4n^2 \equiv -4 \pmod{11}$ is equivalent to $n^2 \equiv -1 \pmod{11}$. This is equivalent to $n^2 \equiv 10 \pmod{11}$. By the division algorithm, all integers can be written as $k + 11 \cdot l$, $k \in \mathbb{Z}_{11}$ and $l \in \mathbb{Z}$; thus it suffices to check all $n \in \mathbb{Z}_{11}$ to see if such an n exists:

$$0^2 \equiv 0 \pmod{11}, \quad 1^2 \equiv 1 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 3^2 \equiv 9 \pmod{11}, \quad 4^2 \equiv 5 \pmod{11}, \quad 5^2 \equiv 4 \pmod{11},$$

$$5^2 \equiv 4 \pmod{11}, \quad 6^2 \equiv 3 \pmod{11}, \quad 7^2 \equiv 5 \pmod{11}, \quad 8^2 \equiv 9 \pmod{11}, \quad 9^2 \equiv 4 \pmod{11}, \quad 10^2 \equiv 1 \pmod{11}.$$

Since no $n \in \mathbb{Z}_{11}$ satisfies the congruence $4 \cdot (n^2 + 1) \equiv 0 \pmod{11}$ we know no such integer n exists. Hence, $4 \cdot (n^2 + 1)$ is never divisible by 11. □

Exercise 3

Exercise 1.3.14 of B & B: Find the units digit of $3^{29} + 11^{12} + 15$.

Proof. To find the units digit we will reduce $3^{29} + 11^{12} + 15 \bmod 10$. Notice,

$$\left(3^{29} + 11^{12} + 15\right) \bmod 10 = 3^{29} \bmod 10 + 11^{12} \bmod 10 + 15 \bmod 10.$$

Now we will reduce each of these integers mod 10:

$$3^{29} \bmod 10 = (3^4)^7 \cdot 3 \bmod 10 = (81)^7 \cdot 3 \bmod 10 = (1)^7 \cdot 3 \bmod 10 = 1 \cdot 3 \bmod 10 = 3 \bmod 10, \tag{2}$$

$$11^{12} \bmod 10 = (1)^{12} \bmod 10 = 1 \bmod 10, \tag{3}$$

and

$$15 \bmod 10 = 5 \bmod 10. \tag{4}$$

Thus,

$$\left(3^{29} + 11^{12} + 15\right) \bmod 10 = 3 \bmod 10 + 1 \bmod 10 + 5 \bmod 10 = (3 + 1 + 5) \bmod 10 = 9 \bmod 10.$$

Hence the units digit of $3^{29} + 11^{12} + 15$ is 9. $\square$

Exercise 4

Exercise 1.3.20 of B & B: Solve the following system of congruences:

$$2x \equiv 5 \pmod 7, \qquad 3x \equiv 4 \pmod 8 \tag{5}$$

First we will solve each of the congruences in equation 5 for x. By trial and error, -3 is found to be an inverse of 2 mod 7 and -5 is found to be an inverse of 3 mod 8. Applying these inverses we have:

$$-3 \cdot 2x \equiv -3 \cdot 5 \pmod 7, \qquad -6x \equiv -15 \pmod 7, \qquad 1 \cdot x \equiv 6 \pmod 7, \qquad x \equiv 6 \pmod 7$$

and

$$-5 \cdot 3x \equiv -5 \cdot 4 \pmod 8 \qquad -15x \equiv -20 \pmod 8 \qquad 1 \cdot x \equiv 4 \pmod 8 \qquad x \equiv 4 \pmod 8.$$

Now, using the construction within the proof of the Chinese Remainder Theorem, we will solve the system of equations, $x \equiv 6 \pmod 7$, $x \equiv 4 \pmod 8$ which we showed is equivalent to the system given in (5). Since $\gcd(7, 8) = 1$, theorem 1.3.6 implies the given system has a solution modulo $7 \cdot 8$. The congruence $x \equiv 6 \pmod 7$ gives us the equation $x = 6 + 7k$ for some integer k. Then, substituting we obtain $6 + 7k \equiv 4 \pmod 8$, or equivalently, $7k \equiv -2 \pmod 8$. Multiplying by 7, Since $7 \cdot 7 \equiv 1 \pmod 8$, gives us $k \equiv -14 \pmod 8$ or $k \equiv 2 \pmod 8$. This yields the particular solution $x = 6 + 7 \cdot 2 = 20$. Thus, we write the solution to the given system of equations, $x \equiv 20 \pmod{56}$.

Exercise 5

Exercise 1.3.24 of B&B: Show that the remainder of an integer n when divided by 9 is the same as the remainder of the sum of its digits when divided by 9.

Proof. We will show for any integer n written in decimal form as $n = a_k a_{k-1} ... a_1 a_0$ satisfies the following equation:

$$n \ \equiv \ (a_k + a_{k-1} + \ \dots \ + a_1 + a_0) \ \text{mod } 9.$$

If n has decimal digits $a_k a_{k-1} ... a_1 a_0$ we can write n in expanded form:

$$n = 10^k \cdot a_k + 10^{k-1} \cdot a_{k-1} + \ \dots \ + 10^1 \cdot a_1 + 10^0 \cdot a_0.$$

If this equality holds, it must also be valid mod 9:

$$n \ \equiv \left(10^k \cdot a_k + 10^{k-1} \cdot a_{k-1} + ... + 10^1 \cdot a_1 + 10^0 \cdot a_0\right) \ \text{mod } 9.$$

Then, since $10 \equiv 1 \pmod 9$, we can write

$$n \ \equiv \left(1^k \cdot a_k + 1^{k-1} \cdot a_{k-1} + ... + 1^1 \cdot a_1 + 1^0 \cdot a_0\right) \ \text{mod } 9.$$

Any power of 1 is 1, so we have

$$n \ \equiv (1 \cdot a_k + 1 \cdot a_{k-1} + ... + 1 \cdot a_1 + 1 \cdot a_0) \ \text{mod } 9.$$

Because 1 is the multiplicative identity, we have

$$n \ \equiv (a_k + a_{k-1} + ... + a_1 + a_0) \ \text{mod } 9.$$

Therefore, when divided by 9, the remainder of n is be the same as the remainder of the sum of its digits. □

Exercise 6

Exercise 1.3.26 of B&B: let p be a prime number and let a, b be any integers. Prove that $(a+b)^p \equiv a^p + b^p \pmod{p}$

Proof. Let p be a prime number and let a, b be any integers. Using the binomial formula,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} \cdot b^k$$

Expanding this binomial we have

$$(a+b)^p = \binom{p}{0} a^p \cdot b^0 + \binom{p}{1} a^{p-1} \cdot b^1 + \binom{p}{2} a^{p-2} \cdot b^2 + \ \dots \ + \binom{p}{p-2} a^2 \cdot b^{p-2} + \binom{p}{p-1} a^1 \cdot b^{p-1} + \binom{p}{p} a^0 \cdot b^p.$$

Notice

$$\binom{p}{0} a^p \cdot b^0 = a^p \qquad \text{and} \binom{p}{p} a^0 \cdot b^p = b^p$$

Thus our goal is to show that for all $1 \leq k \leq p-1$,

$$\binom{p}{k} a^{p-k} \cdot b^k \equiv 0 \pmod{p}.$$

Note

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1)!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!}.$$

The coefficients $\frac{p!}{k!(p-k)!}$ are known to be integers from the binomial theorem. Also, since p is prime, $\frac{p!}{k!(p-k)!}$ has p as a factor because p is a divisor of the numerator but not the denominator. Thus $\frac{(p-1)!}{k!(p-k)!}$ is an integer and $p \mid \binom{p}{k}$ for $1 \leq k \leq p-1$. Since $\binom{p}{0} = \binom{p}{p} = 1$, the coefficients on a^p and b^p are not divisible by p whereas when $1 \leq k \leq p-1$, $\binom{p}{k} \equiv 0 \pmod{p}$. This implies $\binom{p}{k} a^{p-k} \cdot b^k \equiv 0 \pmod{p}$ when $1 \leq k \leq p-1$. Thus,

$$(a+b)^p \equiv \binom{p}{0} a^p \cdot b^0 + 0 + 0 + \ \dots \ + 0 + 0 + \binom{p}{p} a^0 \cdot b^p \pmod{p}$$

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

□

Exercise 7

Exercise 1.4.1(b): Make addition and multiplication tables for the set $\mathbb{Z}_4$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Exercise 8

Exercise 1.4.2(a) in B & B: Make multiplication table for $\mathbb{Z}_6$.

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Exercise 9

Exercise 1.4.3(b) in B & B: Find the multiplicative inverses [38] in $\mathbb{Z}_{83}$.

Since 83 is prime, [38] has multiplicative inverses (by corollary 1.4.6). To find $[38]_{83}^{-1}$, we can use the matrix form of the Euclidean algorithm:

$$\begin{bmatrix}1 & 0 & 83\\0 & 1 & 38\end{bmatrix} \xrightarrow{R_1-2R_2} \begin{bmatrix}1 & -2 & 7\\0 & 1 & 38\end{bmatrix} \xrightarrow{R_2+-5R_1} \begin{bmatrix}1 & -2 & 7\\-5 & 11 & 3\end{bmatrix} \xrightarrow{R_1-2R_2} \begin{bmatrix}11 & -24 & 1\\-5 & 11 & 3\end{bmatrix} \xrightarrow{R_2+-3R_1} \begin{bmatrix}11 & -24 & 1\\-38 & 83 & 0\end{bmatrix}$$

.

Thus, $11 \cdot 83 + -24 \cdot 38 = 1$, which shows that $[38]_{83}^{-1} = [-24]_{83} = [59]_{83}$.

Exercise 10

Exercise 1.4.9(a) in B & B: Let $\gcd(a, n) = 1$. The smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ is called the multiplicative order of $[a]$ in $\mathbb{Z}_n^\times$. Find the multiplicative orders of [2] and [5] in f.

First, note that $\gcd(5, 16) = 1$, so we will find the multiplicative order of [5] in $\mathbb{Z}_{16}^\times$ using theorem 1.4.11. Since $\varphi(16) = 8$, we know that $5^8 \equiv 1 \pmod{16}$. However, by exercise 1.4.10, the multiplicative order of any element of $\mathbb{Z}_{16}^\times$ must divide $\varphi(16) = 8$, so we must test $1, 2, 4, 8$:

$$5^1 \equiv 5 \pmod{16}, \qquad 5^2 \equiv 9 \pmod{16}, \qquad 5^4 \equiv (5^2)^2 \equiv 9^2 \equiv 81 \equiv 1 \pmod{16}.$$

Hence the multiplicative order of [5] in $\mathbb{Z}_{16}^\times$ is 4.

Next, find the multiplicative order of [7] in $\mathbb{Z}_{16}^\times$ by testing $1, 2, 4, 8$:

$$7^1 \equiv 7 \pmod{16}, \qquad 7^2 \equiv 49 \equiv 1 \pmod{16}.$$

Hence the multiplicative order of [7] in $\mathbb{Z}_{16}^\times$ is 2.

Exercise 11

Exercise 1.4.14 from B & B: If p is a prime number, show that $[0]$ and $[1]$ are the only idempotent elements in $\mathbb{Z}_p$.

Proof. Note that $[0]$ is trivially idempotent since 0 times any integer in $\mathbb{Z}_p$ must be zero, so $[0]^2 = [0]$. Suppose there exists some $a \in \mathbb{Z}_p$ such that $[a]^2 = [a]$ but $a > 1$. Since $[a]^2 = [a]$, $a^2 \equiv a \pmod{p}$. Because p is prime, all nonzero elements in $\mathbb{Z}_p$ have a multiplicative inverse. Thus, there exists some integer a^{-1} such that $a^{-1} \cdot a \equiv 1 \pmod{p}$. Multiply both sides of the congruence $a^2 \equiv a \pmod{p}$ by a^{-1} to obtain $a^{-1} \cdot a^2 \equiv a^{-1} \cdot a \pmod{p}$. Equivalently, $a^{-1} \cdot a \cdot a \equiv 1 \pmod{p}$ and $1 \cdot a \equiv 1 \pmod{p}$. Thus, $a \equiv 1 \pmod{p}$ which contradicts our assumption that a is in $\mathbb{Z}_p$ but $a > 1$. Thus, $[0]$ and $[1]$ are the only idempotent elements in $\mathbb{Z}_p$. □

Exercise 12

Exercise 1.4.15 from B & B: If n is not a prime power, show that $\mathbb{Z}_n$ has an idempotent element different from $[0]$ and $[1]$.

Proof. Assume n is not a prime power. Thus, n must have more than one prime factor so there must exist integers b and c such that $b \mid n$, $c \mid n$, $n = bc$, and $\gcd(b, c) = 1$. Because $\gcd(b, c) = 1$, the Chinese Remainder Theorem implies a solution, x, exists mod bc to the following system of congruences:

$$x \equiv 1 \pmod{b}, \qquad x \equiv 0 \pmod{c}.$$

Claim 1: $x \not\equiv 0 \pmod{bc}$

Proof. If $x \equiv 0 \pmod{bc}$, $bc \mid x$ implies $b \mid x$, but $x \equiv 1 \pmod{b}$. □

Claim 2: $x \not\equiv 1 \pmod{bc}$

Proof. If $x \equiv 1 \pmod{bc}$, $bc \mid (x-1)$ implies $c \mid (x-1)$, but $x \equiv 0 \pmod{c}$.

□

Notice if $x \equiv 1 \pmod{b}$ and $x \equiv 0 \pmod{c}$, $x = 1 + bk$ and $x = cm$ for some integers k, m. If we multiply both sides of the equation $x = 1 + bk$ by x we obtain $x \cdot x = (1 + bk)x$. This implies $x^2 = 1 \cdot x + (bk) \cdot x$. Since $x = cm$ t, $x^2 = x + (bk) \cdot cm$. Thus, $x^2 \equiv x \pmod{bc}$.

□

Exercise 13

Exercise 1.4.16 from B & B: An element $[a]$ of $\mathbb{Z}_n$ is said to be nilpotent if $[a]^k = [0]$ for some k. Show that $\mathbb{Z}_n$ has no nonzero nilpotent elements if and only if n has no factor that is a square (except 1).

Proof. First, assume n has no factor that is a square. Then, write the prime factorization of n:

$$n = \prod_{i=1}^{m} p_i^{\alpha_i}, \qquad \text{where } p_i \text{ are prime, } \alpha_i, \text{ are in } \mathbb{Z}^+.$$

But, n has no square factors, so we can conclude that all $\alpha_i = 1$:

$$n = \prod_{i=1}^{m} p_i \qquad \text{where } p_i \text{ are prime.}$$

We want to show that $\mathbb{Z}_n$ has no nonzero nilpotent elements. Suppose that $\mathbb{Z}_n$ has some nonzero nilpotent element, $[a]$, $[a] \neq [0]$. Then, $a^k \equiv 0 \pmod{n}$. This implies $n \mid a^k$. Equivalently, $\prod_{i=1}^{m} p_i \mid a^k$. Then, there exists some integer b such that $a^k = b \cdot (\prod_{i=1}^{m} p_i)$. So, for any $1 \leq j \leq m$,

$$a^k = p_j \cdot b \cdot \prod_{i=1}^{j-1} p_i \cdot \prod_{i=j+1}^{m} p_i.$$

Thus for all $1 \leq j \leq m$, $p_j \mid a^k$. Equivalently, for all $1 \leq j \leq m$, $p_j \mid a \cdot a^{k-1}$. So by corollary 1.2.6, we can inductively conclude that for all $1 \leq j \leq m$, $p_j \mid a$. Hence, $\prod_{i=1}^{m} p_i \mid a$. This contradicts our assumption that $[a] \neq [0]$. Therefore, $\mathbb{Z}_n$ has no nonzero nilpotent elements.

Next, assume $\mathbb{Z}_n$ has no nonzero nilpotent elements. Then, there are no $[a] \neq [0]$ such that $a^k \equiv 0 \pmod{n}$. Suppose n has some square factor, $s^2 \neq 1$, so $n = t \cdot s^2$. Note $[st] \in \mathbb{Z}_n$ and $[st] \neq [0]$ since $n \nmid st$; but $(ts)^2 \equiv 0 \pmod{n}$. Thus, if $\mathbb{Z}_n$ has no nonzero nilpotent elements, n has no square factors.

□

Exercise 14

Exercise 1.4.17 from B & B: Compute $\varphi(27), \varphi(81), \varphi(p^\alpha)$

Using the formula in proposition 1.4.8, since $27 = 3^3$, $\varphi(27) = 27\left(1 - \frac{1}{3}\right) = 18$.
Similarly, $81 = 3^4$, so $\varphi(81) = 81\left(1 - \frac{1}{3}\right) = 54$.
Finally, $\varphi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right) = p^\alpha\left(\frac{p-1}{p}\right) = p^{\alpha-1}(p-1) = p^\alpha - p^{\alpha-1}$.

Give a proof that the formula for $\varphi(n)$ is valid when $n = p^\alpha$.

To calculate $\varphi(p^\alpha)$, we need to count the number of integers from the set $\mathbb{Z}_{p^\alpha}$ that are relatively prime to p^α. Note $|\mathbb{Z}_{p^\alpha}| = p^\alpha$. To find $\varphi(p^\alpha)$, we will first find all integers in $\mathbb{Z}_{p^\alpha}$ that are not relatively prime to p^α. Consider $m \in \mathbb{Z}_{p^\alpha}$ such that $\gcd(m, p^\alpha) \neq 1$. To count how many m exist, we will prove the following lemma.

Lemma 0.1. *The following statements are equivalent when p is prime, $\alpha \in \mathbb{Z}^+$, $m \in \mathbb{Z}^+$ and $1 \leq k < p^\alpha$:*

i. $\gcd(k, p) = 1$
ii. $\gcd(k, p^\alpha) = 1$
iii. k is not a multiple of p

Proof. To show these statements are equivalent, it suffices to prove the following conditional statements:

(1) If $\gcd(k, p) = 1$, then $\gcd(k, p^\alpha) = 1$.
(2) If $\gcd(k, p^\alpha) = 1$, then k is not a multiple of p.
(3) If k is not a multiple of p, then $\gcd(k, p) = 1$.

(1). Assume $\gcd(k, p) = 1$. Note if $\alpha = 2$, proposition 1.2.3 (d) implies $\gcd(k, p^2) = 1$. Now, assume when $\alpha = n$, $\gcd(k, p^n) = 1$. If $\gcd(k, p^n) = 1$ and $\gcd(k, p) = 1$, proposition 1.2.3 (d) implies $\gcd(k, p^{n+1}) = 1$. Thus, by the principle of induction, $\gcd(k, p^\alpha) = 1$ for any $\alpha \in \mathbb{Z}^+$.

(2). Assume $\gcd(k, p^\alpha) = 1$. Then, by theorem 1.1.6 there exists integers x, y such that $kx + p^\alpha y = 1$. Equivalently, $kx + p(p^{\alpha-1}y) = 1$. Again, by theorem 1.1.6, this implies $\gcd(k, p) = 1$. Then, $p \nmid k$ so k is not a multiple of p.

(3). Assume k is not a multiple of p. Then, $p \nmid k$. The only divisors of p are 1 and p so if $p \nmid k$, $\gcd(k, p) = 1$.

By lemma 0.1, we know the following statements are equivalent:

i. $\gcd(k, p) \neq 1$
ii. $\gcd(k, p^\alpha) \neq 1$
iii. k is a multiple of p.

Thus, the only $m \in \mathbb{Z}_{p^\alpha}$ such that $\gcd(m, p^\alpha) \neq 1$, are multiples of p: $0, p, 2p, 3p, ..., p^{\alpha-1}p$. So every p^{th} integer in $\{0, 1, 2, ..., p^\alpha - 1\}$ is a multiple of p. Thus, there are $p^\alpha/p = p^{\alpha-1} m \in \mathbb{Z}_{p^\alpha}$ such that $\gcd(m, p^\alpha) \neq 1$.

Therefore, $\varphi(n) = p^\alpha - p^{\alpha-1}$. □

Exercise 15

Exercise 1.4.24 from B & B: Show that if p is a prime number, then the congruence $x^2 \equiv 1 \pmod{p}$ has only the solutions $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$.

Proof. Let p be a prime number and let $x \in \mathbb{Z}_p$ such that $x^2 \equiv 1 \pmod{p}$. Note that $x \equiv 1$ and $x \equiv -1$ satisfy the given congruence since $1^2 \equiv 1 \pmod{p}$ and $(-1)^2 \equiv 1 \pmod{p}$. Now, suppose there exists some other integer a such that $a^2 \equiv 1 \pmod{p}$ but $a \not\equiv 1, -1$. Then, $a^2 - 1 \equiv 0 \pmod{p}$, or equivalently, $(a-1)(a+1) \equiv 0 \pmod{p}$. Thus, $p \mid (a-1)(a+1)$. By corollary 1.2.6 in B & B, if $p \mid (a-1)(a+1)$, then $p \mid (a-1)$ or $p \mid (a+1)$. if $p \mid (a-1)$, then $a - 1 \equiv 0 \pmod{p}$ which implies $a \equiv 1 \pmod{p}$ which contradicts our assumption that $a \not\equiv 1$. If $p \mid (a+1)$, $a + 1 \equiv 0 \pmod{p}$ which implies $a \equiv -1 \pmod{p}$ which contradicts our assumption that $a \not\equiv -1$. Thus, the congruence $x^2 \equiv 1 \pmod{p}$ has only the solutions $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$. □

Exercise 16

Exercise 1.4.27 from B & B: Show that if p is a prime number, then $(p-1)! \equiv -1 \pmod p$.

Proof. Let p be a prime number. Note that when $p = 2$ and $p = 3$, $(2-1)! \equiv 1! \equiv -1 \pmod 2$ and $(3-1)! \equiv 2! \equiv\equiv 2 \equiv -1 \pmod 3$. We have shown the given congruence holds for $p = 2, 3$, so we will consider only $p > 3$ and so that p is odd. Consider $[a]_p$. Since every integer $1 \leq a \leq p-1$ is relatively prime to p, all $[a]_p$ have unique multiplicative inverses in $\mathbb{Z}_p$. Thus, $(p-1)!$ is the product of all elements in $\mathbb{Z}_p^\times$. So for all $[a]_p$ we can find a unique $[a]_p^{-1}$. Note that the only cases when $[a]_p^{-1} = [a]_p$ can be found by applying exercise 24 in section 1.4 of B & B: if the only solutions to $a^2 \equiv 1 \pmod p$ are ± 1, then $a^{-1}a^2 \equiv a^{-1}1 \pmod p$ implies ± 1 are the only solutions to $a \equiv a^{-1} \pmod p$. Thus for all $a \neq 1, p-1$ in $\mathbb{Z}_p$ there exists a unique a^{-1} in $\mathbb{Z}_p$ with $a \neq a^{-1}$. Then all $2 \leq a \leq p-2$ must have a multiplicative inverse $2 \leq a^{-1} \leq p-2$. Consider the product $2 \cdot 3 \cdot 4 \cdots (p-3)(p-2)$ then rearrange and group this product so that each element is multiplied by its multiplicative inverse so that $2 \cdot 3 \cdot 4 \cdots (p-3)(p-2) \equiv 1 \pmod p$. Then, multiply both sides by $p-1$ to obtain $2 \cdot 3 \cdot 4 \cdots (p-3)(p-2)(p-1) \equiv 1(p-1) \pmod p$, or equivalently, $1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-3)(p-2)(p-1) \equiv -1 \pmod p$. Thus, $(p-1)! \equiv -1 \pmod p$ when p is prime.

□