Math 110 Problem Set 1 Solutions

April 14 2018

**Problem 1** (HPS 1.9 (a), (b)). Use the Euclidean algorithm to compute the following greatest common divisors.

(a) gcd(291, 252).

(b) gcd(16261, 85652).

**Solution.** (a) Using the Euclidean algorithm, we have

\[
\begin{align*}
291 &= 252 \cdot 1 + 39 \\
252 &= 39 \cdot 6 + 18 \\
39 &= 18 \cdot 2 + \underline{3} \\
8 &= 6 \cdot 3 + 0.
\end{align*}
\]

So gcd(291, 252) = 3.

(b) Using the Euclidean algorithm, we have

\[
\begin{align*}
85652 &= 16261 \cdot 5 + 4347 \\
16261 &= 4347 \cdot 3 + 3220 \\
4347 &= 3220 \cdot 1 + 1127 \\
3220 &= 1127 \cdot 2 + 966 \\
1127 &= 966 \cdot 1 + \underline{161} \\
966 &= 161 \cdot 6 + 0
\end{align*}
\]

So gcd(16261, 85652) = 161.

**Problem 2** (HPS 1.10 (a), (b)). For each of the gcd(a, b) values in Problem 1, use the extended Euclidean algorithm to find integers u and v such that au + bv = gcd(a, b).
Solution. (a) From Problem 1 (a), we have
\[
\gcd(291, 252) = 3 = 39 - 18 
\cdot 2
= 39 - (252 - 39 \cdot 6) \cdot 2
= 39 \cdot 13 - 252 \cdot 2
= (291 - 252) \cdot 13 - 252 \cdot 2
= 291 \cdot 13 - 252 \cdot 15.
\]
So we have \(291 \cdot 13 - 252 \cdot 15 = 3\), i.e. \(u = 13, v = -15\).

(b) From Problem 1 (b), we have
\[
\gcd(16261, 85652) = 161 = 1127 - 966 
\cdot 1
= 1127 - (3220 - 1127 \cdot 2) \cdot 1
= 1127 \cdot 3 - 3220
= (4347 - 3220) \cdot 3 - 3220
= 4347 \cdot 3 - (16261 - 4347 \cdot 3) \cdot 4
= 16261 \cdot 4 - 4347 \cdot 15 - 16261 \cdot 4
= (85652 - 16261 \cdot 5) \cdot 15 - 16261 \cdot 4
= 85652 \cdot 15 - 16261 \cdot 79.
\]
So we have \(-16261 \cdot 79 + 85652 \cdot 15 = 161\), i.e. \(u = -79, v = 15\).

Problem 3 (HPS 1.11). Let \(a\) and \(b\) be positive integers.

(a) Suppose that there are integers \(u\) and \(v\) satisfying \(au + bv = 1\). Prove that \(\gcd(a, b) = 1\).

(b) Suppose that there are integers \(u\) and \(v\) satisfying \(au + bv = 6\). Is it necessarily true that \(\gcd(a, b) = 6\)? If not, give a specific counterexample, and describe in general all of the possible values of \(\gcd(a, b)\)?

(c) Suppose that \((u_1, v_1)\) and \((u_2, v_2)\) are two solutions in integers to the equation \(au + bv = 1\). Prove that \(a\) divides \(v_2 - v_1\) and that \(b\) divides \(u_2 - u_1\).

(d) More generally, let \(g = \gcd(a, b)\) and let \((u_0, v_0)\) be a solution in integers to \(au + bv = g\). Prove that every other solution has the form \(u = u_0 + kb/g\) and \(v = v_0 - ka/g\) for some integer \(k\). (This is the second part of Theorem 1.11.

Solution. (a) Suppose that there exist \(u, v \in \mathbb{Z}\) such that \(au + bv = 1\). Let \(c\) be any integer that divides both \(a\) and \(b\). Then \(c|au, c|bv\), so \(c|au + bv = 1\). Hence \(c = \pm 1\), so the greatest common divisor of \(a\) and \(b\) must be 1.

(b) It is not necessarily true; for a counterexample, let \(a = 2, b = 4\): we have \(a \cdot 1 + b \cdot 1 = 6\), but \(6 \nmid a, b\), so \(\gcd(a, b) \neq 6\). More generally, let \(g = \gcd(a, b)\). We have \(gcd|a, b\), so \(gcd|au + bv = g\). Hence the possible values for \(\gcd(a, b)\) are 1, 2, 3, and 6. Examples of each of these possibilities are in the table below:

<table>
<thead>
<tr>
<th>((a, b))</th>
<th>((u, v)) s.t. (au + bv = 1)</th>
<th>(\gcd(a, b))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1, 5)</td>
<td>(1, 1)</td>
<td>1</td>
</tr>
<tr>
<td>(2, 4)</td>
<td>(1, 1)</td>
<td>2</td>
</tr>
<tr>
<td>(3, 6)</td>
<td>(0, 1)</td>
<td>3</td>
</tr>
<tr>
<td>(6, 6)</td>
<td>(1, 0)</td>
<td>6</td>
</tr>
</tbody>
</table>
(c) We have
\[ au_1 + bv_1 = 1, \]
\[ au_2 + bv_2 = 1. \]
Subtract the second equation from the first to get
\[ a(u_1 - u_2) + b(v_1 - v_2) = 0 \]
\[ \implies a(u_1 - u_2) = b(v_2 - v_1). \]
So \(a|b(v_2 - v_1)\) and \(b|a(u_1 - u_2)\). Since \(a, b\) are relatively prime, we must have \(a|v_2 - v_1\) and \(b|u_2 - u_1\).

(d) First, note that \(a(u_0 + kb/g) + b(v_0 - ka/g) = au_0 + kab/g + bv_0 - kab/g = au_0 + bv_0 = g\), so that \(u = u_0 + kb/g, v = v_0 - ka/g\) is indeed a solution to \(au + bv = g\). Conversely, suppose that \(au + bv = g\). As in part (c), we have
\[ a(u - u_0) = b(v - v_0). \]
Since \(g|a, b\), we have \(a = gx, b = gy\) for some integers \(x, y\), so we have
\[ gx(u - u_0) = gy(v - v_0) \]
\[ \implies x(u - u_0) = y(v - v_0). \]
Since \(g\) is the greatest common divisor of \(a, b, x\) and \(y\) must be relatively prime, so \(x|v - v_0, y|u - u_0\), so we have
\[ u - u_0 = yr \]
\[ v - v_0 = xs \]
for some integers \(r, s\). Hence we have
\[ u = yr + u_0 = \frac{b}{g}r + u_0 \]
\[ v = xs + v_0 = \frac{a}{g}s + v_0. \]
Substituting these values into the equation \(au + bv = g\), we have
\[ a\left(b\frac{r}{g} + u_0\right) + b\left(a\frac{s}{g} + v_0\right) = g \]
\[ \implies abr/g + abs/g + (au_0 + bv_0) = g \]
\[ \implies abr/g + abs/g = 0 \]
\[ \implies s = -r. \]
So if we let \(k = r = -s\), we have \(u = u_0 + kb/g, v = v_0 - ka/g\).
Problem 4 (HPS 1.16). Do the following modular computations. In each case, fill in the box with an integer between 0 and $m - 1$, where $m$ is the modulus.

(a) $347 + 513 \equiv \underline{97}$ mod 763.

(b) $3274 + 1238 + 7231 + 6437 \equiv \underline{8926}$ mod 9254.

(c) $153 \cdot 287 \equiv \underline{139}$ mod 353.

(d) $357 \cdot 862 \cdot 193 \equiv \underline{636}$ mod 943.

(e) $5327 \cdot 6135 \cdot 7139 \cdot 2187 \cdot 5219 \cdot 1873 \equiv \underline{603}$ mod 8157. (Hint. After each multiplication, reduce modulo 8157 before doing the next multiplication.)

(f) $137^2 \equiv \underline{130}$ mod 327.

(g) $373^6 \equiv \underline{463}$ mod 581.

(h) $23^3 \cdot 19^5 \cdot 11^4 \equiv \underline{93}$ mod 97.

Solution. (a) 97

(b) 8926

(c) 139

(d) 636

(e) 603

(f) 130

(g) 463

(h) 93

Problem 5 (HPS 1.17). Find all values of $x$ between 0 and $m - 1$ that are solutions of the following congruences. (Hint. If you can’t figure out a clever way to find the solution(s), you can just substitute each value $x = 1, x = 2, \ldots, x = m - 1$ and see which ones work.)

(a) $x + 17 \equiv 23$ mod 37.

(b) $x + 42 \equiv 19$ mod 51.

(c) $x^2 \equiv 3$ mod 11.

(d) $x^2 \equiv 2$ mod 13.
(e) \( x^2 \equiv 1 \mod 8 \).

(f) \( x^3 - x^2 + 2x - 2 \equiv 0 \mod 11 \).

(g) \( x \equiv 1 \mod 5 \) and also \( x \equiv 2 \mod 7 \). (Find all solutions modulo 35, that is, find the solutions satisfying \( 0 \leq x \leq 34 \).

**Solution.**

(a) \( x \equiv 23 - 17 \equiv 6 \mod 37 \).

(b) \( x \equiv 19 - 42 \equiv 19 + 9 \equiv 28 \mod 51 \).

(c) \( x \equiv 5 \mod 11 \) or \( x \equiv 6 \mod 11 \).

(d) No solutions: 2 is not a square modulo 13.

(e) \( x \equiv 1, 3, 5, \) or 7 \mod 8 \).

(f) \( x \equiv 1, 3, \) or 8 \mod 11 \).

(g) \( x \equiv 16 \mod 35 \).

**Problem 6** (HPS 1.18). Suppose that \( g^a \equiv 1 \mod m \) and that \( g^b \equiv 1 \mod m \). Prove that \( g^{gcd(a,b)} \equiv 1 \mod m \).

**Solution.** By Bézout’s Lemma, there exist integers \( u, v \) such that \( au + bv = gcd(a, b) \). Then we have

\[
g^{gcd(a,b)} \equiv g^{au+bv} \mod m \\
\equiv (g^a)^u \cdot (g^b)^v \mod m \\
\equiv 1^u \cdot 1^v \mod m \\
\equiv 1 \mod m.
\]

Note that \( g \) is invertible \mod m as \( g^a \equiv 1 \mod m \), so we don’t have to worry about negative powers of \( g \): we know they exist.

**Problem 7** (HPS 1.20). Prove that \( m \) is prime if and only if \( \phi(m) = m - 1 \), where \( \phi \) is Euler’s phi function.

**Solution.** Euler’s phi function \( \phi(m) \) counts the number of integers in the range \([1, m - 1]\) that are relatively prime to \( m \). If \( m \) is prime, then these are all relatively prime to \( m \), so that \( \phi(m) = \#[1, m - 1] = m - 1 \). Conversely, suppose \( \phi(m) = m - 1 \). This is \( \#[1, m - 1] \), so this means that every integer in \([1, m - 1]\) is relatively prime to \( m \). In particular, only 1 can divide \( m \). Hence \( m \) is prime.
Problem 8 (HPS 1.22). Let \( m \) be an odd integer and let \( a \) be any integer. Prove that \( 2m + a^2 \) can never be a perfect square. (Hint. If a number is a perfect square, what are its possible values modulo 4?)

Solution. The residues modulo 4 are 0, 1, 2, 3, and their squares are 0, 1, 0, 1, respectively. Hence every square number is congruent to 0 or 1 modulo 4. Since \( m \) is an odd integer, \( m \equiv 1 \mod 4 \) or \( m \equiv 3 \mod 4 \). Multiplying by 2, we have \( 2m \equiv 2 \mod 4 \). From the above calculation, we know that \( a^2 \equiv 0 \mod 4 \) or \( a^2 \equiv 1 \mod 4 \). Hence \( 2m + a^2 \equiv 2 \mod 4 \) or \( 2m + a^2 \equiv 3 \mod 4 \), neither of which is a square modulo 4. Hence \( 2m + a^2 \) is never a perfect square.

Problem 9 (HPS 1.25). Use the square-and-multiply algorithm described in Section 1.3.2, or the more efficient version in Exercise 1.24, to compute the following powers.

(a) \( 17^{183} \mod 256 \).
(b) \( 2^{477} \mod 1000 \).
(c) \( 11^{507} \mod 1237 \).

Solution. (a) 113.
(b) 272.
(c) 322.

Problem 10 (HPS 1.30). For each of the following primes \( p \) and numbers \( a \), compute \( a^{-1} \mod p \) in two ways: (i) Use the extended Euclidean algorithm. (ii) Use the fast power algorithm and Fermats little theorem. (See Example 1.28.)

(a) \( p = 47 \) and \( a = 11 \).
(b) \( p = 587 \) and \( a = 345 \).
(c) \( p = 104801 \) and \( a = 78467 \).

Solution. (a) \( 11^{-1} \equiv 30 \mod 47 \).
(b) \( 345^{-1} \equiv 114 \mod 587 \).
(c) \( 78467^{-1} \equiv 1763 \mod 104801 \).
Problem 11. Suppose that \( m \) is odd. Which integer \( k \in [0, m - 1] \) is the multiplicative inverse of \( [2]_m \) (that is, which \( k \) satisfies \( 2k \equiv 1 \pmod{m} \))? Prove your answer.

Solution. The answer is \( k = \frac{m+1}{2} \).

Proof. First, since \( m \) is odd, \( k = \frac{m+1}{2} \) is an integer. Second, we know that \( m > 1 \). Adding \( m \) to both sides gives \( 2m > m + 1 \), so \( m > \frac{m+1}{2} \), so \( k \) is indeed in \([0, m - 1]\). Finally, we compute
\[
2k = 2 \left( \frac{m+1}{2} \right) = 2m + 1 \equiv 1 \pmod{m}.
\]

Problem 12. (a) Let \( p \) be an odd prime number and consider the squaring mod \( p \) function
\[
s_p : \mathbb{F}_p \rightarrow \mathbb{F}_p,
\]
\[
[x]_p \mapsto [x^2]_p
\]
Prove that the image (aka the range) of \( s_p \) has exactly \( \frac{p+1}{2} \) elements. Hint: Start by showing that \( x^2 \equiv y^2 \pmod{p} \) if and only if \( x \equiv \pm y \pmod{p} \).

(b) Part (a), summarized: “for all primes \( p > 2 \), roughly half the residues \pmod{p} are squares.” Is the statement “for all primes \( p > 3 \), roughly one third of the residues \pmod{p} are cubes” true or false? Explain.

Solution. (a) Following the hint: if \( x \equiv \pm y \pmod{p} \), then \( x^2 \equiv y^2 \pmod{p} \) since multiplication \pmod{p} is well defined. Conversely, suppose that \( x^2 \equiv y^2 \pmod{p} \). We have
\[
x^2 \equiv y^2 \pmod{p} \\
\implies x^2 - y^2 \equiv 0 \pmod{p} \\
\implies (x + y)(x - y) \equiv 0 \pmod{p}.
\]
Now \( p \) is prime, so \( \mathbb{Z}/p\mathbb{Z} \) has no zero divisors, i.e. if \( ab \equiv 0 \pmod{p} \), then one of \( a \) and \( b \) must be congruent to \( 0 \pmod{p} \). This means that either \( x + y \equiv 0 \pmod{p} \), or \( x - y \equiv 0 \pmod{p} \). Hence \( x \equiv \pm y \pmod{p} \).

This allows us to count the possible values for \([x^2]_p\), as follows. We need to account for the squares of all the residues \pmod{p}, i.e. \( 0^2, 1^2, \ldots, (p-1)^2 \). The values of \( 0^2, 1^2, 2^2, \ldots, \left( \frac{p-1}{2} \right)^2 \) must all be different \pmod{p}, since no two \( x, y \) of these numbers, with \( x \neq y \), satisfy \( x \equiv \pm y \pmod{p} \). There are \( \frac{p-1}{2} + 1 = \frac{p+1}{2} \) of these squares \pmod{p}. However, the values of the remaining squares will be equal to some value of one of these squares, since we have
\[
(p-1)^2 \equiv 1^2 \pmod{p}, \quad (p-2)^2 \equiv 2^2 \pmod{p}, \ldots,
\]
since \( x \equiv \pm y \mod p \implies [x^2]_p = [y^2]_p \). Hence we have a total of \( \frac{p+1}{2} \) values in the image of \( s_p \).

(b) This is not true: to prove this, we need a counterexample. Suppose that \( p = 5 \), so \( p \) is a prime greater than 3. Now

\[
\begin{align*}
[0^3]_5 &= [0]_5 \\
[1^3]_5 &= [1]_5 \\
[2^3]_5 &= [8]_5 = [3]_5 \\
[3^3]_5 &= [27]_5 = [2]_5 \\
[4^3]_5 &= [64]_5 = [4]_5.
\end{align*}
\]

So every residue mod 5 is a cube, not only about a third of them: the statement is false.

---

**Problem 13.**  
(a) Let \( n \geq 2 \). Prove that \((n-1)! \equiv -1 \mod n\) if and only if \( n \) is prime.

(b) A primality test is an algorithm that on input \( n \geq 2 \) determines whether \( n \) is PRIME or COMPOSITE. Do you think that checking \((n-1)! \equiv 1 \mod n\) will yield an efficient primality test? Explain.

**Solution.**  
(a) Suppose that \((n-1)! \equiv -1 \mod n\). This means that \((n-1)!\) is relatively prime to \( n \), since \(-1\) is relatively prime to \( n \). In particular, none of \( 2, 3, \ldots, n-1 \) can divide \( n \), since then they would not be relatively prime to \( n \). Hence the only positive integer less than \( n \) that divides \( n \) is 1, i.e. \( n \) is prime.

Conversely, suppose that \( n \) is prime. If \( n = 2 \), we have \((n-1)! = 1 \equiv -1 \mod 2\), so this is true for \( n = 2 \). We now prove this for \( n \) an odd prime; there are several ways we can prove that \((n-1)! \equiv -1 \mod n\).

**Method 1:** We want to take pairs of residues \(a, a^{-1} \mod n\). Suppose that \( a^{-1} \equiv a \mod n\). Then \( a^2 \equiv 1 \mod n\), so from Problem 12 (a), this means that \( a \equiv \pm 1 \mod n\). For all other \( a \in [1, n-1] \), we have \( a \not\equiv a^{-1} \mod n\). Hence the invertible residues mod \( n \) are 1, \(-1\), and pairs of the form \(a, a^{-1}\).

If we take the product of each pair, we get 1. So the product of all the invertible residues mod \( n \) is \(-1 \cdot 1 \cdot \ldots \cdot 1 \mod n\). Hence

\[
(n-1)! \equiv 1 \cdot 2 \cdot \ldots \cdot (n-1) \mod n
\]

\[
\equiv -1 \mod n.
\]

**Method 2:** We can use primitive roots to prove this. Let \( x \) be a primitive root mod \( n \), so that we can write the residues \([1]_n, [2]_n, \ldots, [n-1]_n\) as

\([x]_n, [x^2]_n, \ldots, [x^{n-2}]_n, [x^{n-1}]_n\). Then we have

\[
(n-1)! \equiv x \cdot x^2 \cdot x^3 \cdot \ldots \cdot x^{n-2} \cdot x^{n-1} \mod n
\]

\[
\equiv x^{1+2+\ldots+(n-1)} \mod n
\]

\[
\equiv x^{n(n-1)/2} \mod n.
\]
By Fermat’s Little Theorem, \( x^n \equiv x \mod n \), so we have

\[
(n - 1)! \equiv x^{n(n-1)/2} \mod n
\]
\[
\equiv (x^n)^{(n-1)/2} \mod n
\]
\[
\equiv x^{(n-1)/2} \mod n.
\]

If we square this, we get \((x^{(n-1)/2})^2 = x^{n-1} \equiv 1 \mod n\), by Fermat’s little theorem, so from Problem 12 (a), \( x^{(n-1)/2} \equiv \pm 1 \mod n \). However, it cannot be 1, since \( x \) is a primitive root mod \( n \), so its powers from \( x^1 \) to \( x^{n-1} \) are precisely the distinct nonzero residues mod \( n \), i.e. they are all different. In particular, \( x^{(n-1)/2} \neq x^{n-1} \equiv 1 \mod n \). Hence it must be \(-1\), i.e.

\[
(n - 1)! \equiv x^{(n-1)/2} \mod n
\]
\[
\equiv -1 \mod n.
\]

**Method 3:** We can exploit Lagrange’s theorem to prove this. Define the polynomial function

\[
f(x) = (x - 1)(x - 2)\ldots(x - (n - 1)).
\]

This has exactly \( n - 1 \) roots, namely 1, 2, \ldots, \( n - 1 \). Now define the polynomial function

\[
g(x) = x^{n-1} - 1.
\]

By Fermat’s little theorem, for \( x = 1, 2, \ldots, n - 1 \), we have

\[
x^{n-1} - 1 \equiv 1 - 1 \mod n
\]
\[
\equiv 0 \mod n.
\]

So \( g \) has exactly \( n - 1 \) roots mod \( n \). Note that both \( f \) (think about multiplying it out) and \( g \) both have leading term \( x^{n-1} \). Consider the polynomial \( h(x) = f(x) - g(x) \). Since \( f \) and \( g \) have the same leading term \( x^{n-1} \), the leading term of \( h \) must have degree less than \( n - 1 \), but \( h \) still has \( n - 1 \) roots, the same as \( f \) and \( g \). Lagrange’s theorem in number theory states that the number of roots of a nonzero polynomial over a field \( \mathbb{Z}/p\mathbb{Z} \) for prime \( p \) cannot exceed the degree, but \( h \) has degree less than \( n - 1 \) and also has \( n - 1 \) roots. Hence \( h \) must be zero in the field \( \mathbb{Z}/n\mathbb{Z} \), i.e. \( h(x) \equiv 0 \mod n \).

In particular, the constant term of \( h \) is congruent to 0 mod \( n \). We can compute the constant term directly as follows. The constant term of \( f \) is \(-1 \cdot -2 \cdot \ldots \cdot (n - 1) = (n - 1)!\), since there is an even number of \(-\) signs because \( n \) is odd. The constant term of \( g \) is \(-1\). Hence the constant term of \( h = f - g \) is \((n - 1)! + 1\), so we have

\[
(n - 1)! + 1 \equiv 0 \mod n
\]
\[
\implies (n - 1)! \equiv -1 \mod n.
\]
**Method 4:** If you are familiar with the symmetric groups and the Sylow theorems from group theory, we can use these to prove this. Consider the symmetric group $S_n$. The elements of order $n$ are the $n$-cycles, of which there are $(n-1)!$. Let $N$ be the number of distinct Sylow $n$-subgroups: each is cyclic of order $n$ and has $(n-1)$ elements of order $n$. Their pairwise intersection must be trivial, since the only subgroup of $C_p$ besides $C_p$ itself is the trivial one. These must account for all the elements of order $n$, so we have

\[(n-1)N \equiv n-1 \pmod{n},\]

so multiplying by $(n-1)$, we have

\[(n-1)(n-2)! \equiv n-1 \pmod{n}.\]

(b) This is a very inefficient test for primality, since it involves computing $(n-1)! \pmod{n}$. In fact, even trial division is more efficient, the Euclidean algorithm even more so.

**Problem 14.** The binomial theorem tells us how to expand the two-variable polynomial $(x+y)^n$:

\[
\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k
\]

where the $(n,k)$-th binomial coefficient is given by the formula(s)

\[
\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot \ldots \cdot 1}{k \cdot (k-1) \cdot \ldots \cdot 1} = \left\lfloor \text{number of ways to select an (unordered) subset of } k \text{ (distinct) items from a set of } n \text{ distinct items} \right\rfloor
\]

where $!$ is the factorial.

Prove that if $p$ is prime, then $p \mid \binom{p}{k}$ whenever $1 \leq k \leq p-1$. Explain why

\[(x+y)^p \equiv x^p + y^p \pmod{p}
\]

for all primes $p$. As an example, $(x+y)^3 \equiv x^3 + 3x^2y + 3xy^2 + y^3 \equiv x^3 + y^3 \pmod{3}$.

**Solution.** Suppose that $p$ is prime, and consider the quotient $\frac{p^k}{k!(p-k)!} = \binom{p}{k}$ for $1 \leq k \leq p-1$. Since $1 \leq k \leq p-1$ and $p$ is prime, $p \nmid 1, 2, \ldots, k$. Recall that a number $n$ is prime if and only if $n \mid ab \implies n \mid a$ or $n \mid b$. Since $p$ is prime and does not divide $1, 2, \ldots, k$, it does not divide their product, i.e. $p \nmid 1 \cdot 2 \cdot \ldots \cdot k = k!$. Similarly, since $1 \leq k \leq p-1$, we also have $1 \leq p-k \leq p-1$, and so we have $p \nmid (p-k)!$. Again applying the above, this means that $p \nmid k!(p-k)!$. However, $p \mid p!$. Hence $p$ must divide the quotient $\frac{p^k}{k!(p-k)!}$, i.e. $p \mid \binom{p}{k}$. 

10
Now consider the polynomial \((x + y)^p\). By the binomial theorem, we have
\[
(x + y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k.
\]
But we know that \(p|\binom{p}{k}\), so every term in the sum is congruent to 0 mod \(p\), so we have
\[
(x + y)^p \equiv x^p + y^p \mod p.
\]

**Problem 15.** Alice and Bob are sending each other science fiction novels over an unsecure channel using an affine cipher (sec. 1.7, pg. 43 of HPS). Eve manages to retrieve the following ciphertext:

<table>
<thead>
<tr>
<th>OGRAP</th>
<th>HVRMX</th>
<th>KMETJ</th>
<th>ORMBX</th>
<th>OROGX</th>
</tr>
</thead>
<tbody>
<tr>
<td>OJOPP</td>
<td>MCRWP</td>
<td>ERTJD</td>
<td>LOGDL</td>
<td>JUJPW</td>
</tr>
<tr>
<td>ELYRE</td>
<td>WPBOG</td>
<td>ERXML</td>
<td>KBLOJ</td>
<td>JULVR</td>
</tr>
<tr>
<td>JALVR</td>
<td>OGRFP</td>
<td>TKOXL</td>
<td>KUXOG</td>
<td>JERFX</td>
</tr>
<tr>
<td>LKJLK</td>
<td>FNFLK</td>
<td>MKPDX</td>
<td>JOGRJ</td>
<td>NFCPA</td>
</tr>
<tr>
<td>PWFNR</td>
<td>ILAR</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Suppose Eve knows that the first word of the plaintext is ‘The’ (a lucky, but educated guess). What is the key \(k = (k_1, k_2)\) for the affine cipher Alice and Bob are using? Hint: Remember that \(k_1\) must be relatively prime with 26.

2. Decrypt the last 15 characters of the ciphertext JNFCPAPWFNRILAR and convert them to English plaintext.

**Solution.** (a) We are given that the code sends T to O, H to G, and E to R, i.e.

\[
e_k(20) = 15
\]
\[
e_k(8) = 7
\]
\[
e_k(5) = 18.
\]

Using the definition of an affine cipher, this gives the equations
\[
20k_1 + k_2 \equiv 15 \mod 26
\]
\[
8k_1 + k_2 \equiv 7 \mod 26
\]
\[
5k_1 + k_2 \equiv 18 \mod 26.
\]

Subtracting the third equation from the second, we obtain
\[
3k_1 \equiv 15 \mod 26
\]
\[
\implies k_1 \equiv 5 \mod 26.
\]

We got pretty lucky here: we didn’t even have to compute \(3^{-1}\) mod 26. Substituting back into the second equation, we have
\[
40 + k_2 \equiv 7 \mod 26
\]
\[
\implies k_2 \equiv 19 \mod 26.
\]

So the key \(k = (k_1, k_2)\) they’re using is \((5, 19)\).
(b) We have the decryption of an affine cipher $d_k(c) = k_1^{-1} \cdot (c - k_2)$, where $c$ is the ciphertext. The inverse of 5 modulo 26 is 21, so we have

$$d_k(c) = [21 \cdot (c - 19)]_{26}.$$ 

Applying this to the ciphertext JNFCPAPWFNRILAR, we obtain SYMBOLOFMYEXILE. (Presumably Eve then uses Google to discover that this plaintext is an excerpt from Gene Wolf’s *The Shadow of the Torturer.*)