CS 280 - Homework 4
Solutions

1. Let a, b, and c be positive integers with a and b being coprime.

`i)` Prove that $a|\,bc \implies a|\,c$.

□ Since a and b are coprime, $\gcd(a,b) = 1$. Thus there must exist integers s and t such that $as + bt = 1$. (1) Also, since $a|\,bc$, there must exist an integer r such that $ar = bc$. (2)

$$\begin{aligned} as + bt &= 1 && (1) \\ c(as + bt) &= c \\ cas + cbt &= c \\ cas + (ar)t &= c && (2) \\ a(cs + rt) &= c \\ ak &= c && [k = cs + rt] \end{aligned}$$

Thus, since $ak = c$, $a|\,c$. ■

The most common problem on this question was to argue as follows: Since $a|\,bc$, $\exists\ k \in \mathbb{Z}$ such that $ak = bc$. Since a and b are coprime, it follows that $\exists\ r$ such that $k = rb$, or $b|\,k$. The flaw in this approach lies in the last step. The last assertion ("it follows that ...") is equivalent to the statement that for a, b coprime, $b|\,ak \implies b|\,k$. But this is just a restatement of the original claim; to assert *this* claim, you need to prove the original problem.

`ii)` Prove that $a|\,c \wedge b|\,c \implies ab|\,c$.

□ Again, since a and b are coprime, $\gcd(a,b) = 1$. Thus there must exist integers s and t such that $as + bt = 1$. (1) Note that since $a|\,c$ and $b|\,c$, there must exist integers r and q such that $ar = c$ and $bq = c$. (2)

$$\begin{aligned} as + bt &= 1 && (1) \\ c(as + bt) &= c \\ cas + cbt &= c \\ (bq)as + (ar)bt &= c && (2) \\ ab(qs + rt) &= c \\ ak &= c && [k = qs + rt] \end{aligned}$$

Thus, since $abk = c$, $ab|\,c$. ■

`iii)` Prove that $a^{-1} \equiv s \pmod{b}$ if $as + bt = 1$.

□

$$\begin{aligned} as + bt &= 1 \\ (as + bt) \bmod b &= 1 \bmod b \\ (as) \bmod b + (bt) \bmod b &= 1 \bmod b \\ as \bmod b &= 1 \bmod b && [bt \bmod b = 0] \\ as &\equiv 1 \pmod{b} \\ a^{-1}as &\equiv a^{-1} \pmod{b} \\ s &\equiv a^{-1} \pmod{b} \end{aligned}$$

Thus the claim is proved. ■

For completeness, you should include the last two lines of this proof, rather than simply concluding that $as \equiv 1 \pmod{b}$.

2. `i)` Use the matrix layout algorithm shown in class to find $\gcd(7245, 4784)$, and express it in the form $7245s + 4784t$.

□ The matrix layout algorithm for $\gcd(7245, 4784)$ proceeds as follows:

$$\left(\begin{array}{cc|c} 1 & 0 & 7245 \\ 0 & 1 & 4784 \end{array}\right) \xrightarrow{r_1 = r_1 - r_2} \left(\begin{array}{cc|c} 1 & -1 & 2461 \\ 0 & 1 & 4784 \end{array}\right) \xrightarrow{r_2 = r_2 - r_1}$$
$$\left(\begin{array}{cc|c} 1 & -1 & 2461 \\ -1 & 2 & 2323 \end{array}\right) \xrightarrow{r_1 = r_1 - r_2} \left(\begin{array}{cc|c} 2 & -3 & 138 \\ -1 & 2 & 2323 \end{array}\right) \xrightarrow{r_2 = r_2 - 16r_1}$$
$$\left(\begin{array}{cc|c} 2 & -3 & 138 \\ -33 & 50 & 115 \end{array}\right) \xrightarrow{r_1 = r_1 - r_2} \left(\begin{array}{cc|c} 35 & -53 & 23 \\ -33 & 50 & 115 \end{array}\right) \xrightarrow{r_2 = r_2 - 5r_1}$$
$$\left(\begin{array}{cc|c} \mathbf{35} & \mathbf{-53} & \mathbf{23} \\ -208 & 315 & 0 \end{array}\right)$$

Thus $7245 \cdot 35 + 4784 \cdot (-53) = 23$, and we have $\gcd(7245, 4784)$, $s = 35$ and $t = -53$. ■

`ii)` If it exists, give the value of the multiplicative inverse of 91 modulo 237.

□ We first find $\gcd(91, 237)$ by the matrix layout algorithm:

$$\left(\begin{array}{cc|c} 1 & 0 & 91 \\ 0 & 1 & 237 \end{array}\right) \xrightarrow{r_2 = r_2 - 2r_1} \left(\begin{array}{cc|c} 1 & 0 & 91 \\ -2 & 1 & 55 \end{array}\right) \xrightarrow{r_1 = r_1 - r_2}$$
$$\left(\begin{array}{cc|c} 3 & -1 & 36 \\ 2 & -1 & 55 \end{array}\right) \xrightarrow{r_2 = r_2 - r_1} \left(\begin{array}{cc|c} 3 & -1 & 36 \\ -5 & 2 & 19 \end{array}\right) \xrightarrow{r_1 = r_1 - r_2}$$
$$\left(\begin{array}{cc|c} 8 & -3 & 17 \\ -5 & 2 & 19 \end{array}\right) \xrightarrow{r_2 = r_2 - r_1} \left(\begin{array}{cc|c} 8 & -3 & 17 \\ -13 & 5 & 2 \end{array}\right) \xrightarrow{r_1 = r_1 - 8r_2}$$
$$\left(\begin{array}{cc|c} 112 & -43 & 1 \\ -13 & 5 & 2 \end{array}\right) \xrightarrow{r_2 = r_2 - 2r_1} \left(\begin{array}{cc|c} \mathbf{112} & \mathbf{-43} & \mathbf{1} \\ -237 & 91 & 0 \end{array}\right)$$

Thus:

$$\begin{aligned} 1 &= 91 \cdot 112 + 237 \cdot (-43) \\ 1 \bmod 237 &= \big(91 \cdot 112 + 237 \cdot (-43)\big) \bmod 237 \\ 1 \bmod 237 &= \big(91 \cdot 112\big) \bmod 237 + \big(237 \cdot (-43)\big) \bmod 237 \\ 1 &\equiv 91 \cdot 112 \pmod{237} \end{aligned}$$

Thus we find that $[91]^{-1} = [112]$. ■

3. Prove that for any integers a and b, $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

Note that this proof neglects to consider the case when a or b is negative, for clarity. It is trivial to include this. $\square$ Any positive integer can be represented uniquely by its prime factorization as follows, where p_i is the sequence of prime numbers:

$$x = \prod_{i=1}^{\infty} p_i^{\chi_i}$$

We represent a and b in this way:

$$a = \prod_{i=1}^{\infty} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{\infty} p_i^{\beta_i}$$

As given in class, we can represent the gcd and the lcm of two numbers as follows:

$$\gcd(a, b) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)} \qquad \text{lcm}(a, b) = \prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$$

We thus use the fact that $\min(x, y) + \max(x, y) = x + y$ to show:

$$\begin{aligned}
\gcd(a, b) \cdot \text{lcm}(a, b) &= \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)} \cdot \prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)} \\
&= \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)} \cdot p_i^{\max(\alpha_i, \beta_i)} \\
&= \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)} \\
&= \prod_{i=1}^{\infty} p_i^{\alpha_i + \beta_i} \\
&= \prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot p_i^{\beta_i} \\
&= \prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot \prod_{i=1}^{\infty} p_i^{\beta_i} \\
\gcd(a, b) \cdot \text{lcm}(a, b) &= ab
\end{aligned}$$

Thus the claim is proved. $\blacksquare$

4. Let p be prime. Prove that $(p - 1)! \equiv -1 \pmod{p}$.

In the following proof, the equivalence relation $\equiv$ is understood to mean "equivalent $\pmod{p}$." $\square$ Since $p - 1 \equiv -1$, we need only to prove that $(p - 2)! \equiv -1$; together, these will imply that $(p - 1)(p - 2)! = (p - 1)! \equiv -1 \cdot 1 = -1$. To show that $(p - 2)! \equiv -1$, we will first prove that every integer x between 2 and $p - 2$ has a unique inverse such that $x^{-1} \not\equiv x$.

Take an integer $x = p - i$, $2 \leq i \leq p - 2$. We show that x has an inverse as follows. Since p is prime and $x < p$, we know that p and x are coprime, and thus we can write $sx + pt = 1$ for some $s, t \in \mathbb{Z}$. Thus by the solution to 1(iii), we know that $x^{-1} \equiv s$.

To show that $x^{-1} \not\equiv x$, we simply solve for a when a *is* equal to its inverse a^{-1}. By definition, $aa^{-1} \equiv 1$. When $a = a^{-1}$, this is just $a^2 \equiv 1$, or $a \equiv \sqrt{1}$. The two cases for which this is true are $a \equiv 1$ and $a \equiv -1 \equiv p - 1$. Since we know that $2 \leq x \leq p - 2$, we have shown that $x^{-1} \not\equiv x$.

We now show that each inverse is unique. Assume that we have two integers a and b such that $a^{-1} \equiv b^{-1}$. Prove that this implies $a \equiv b$.

$$\begin{aligned} a^{-1} &\equiv b^{-1} \\ aa^{-1} &\equiv ab^{-1} \\ 1 &\equiv ab^{-1} \\ b &\equiv ab^{-1}b \\ b &\equiv a \end{aligned}$$

Thus if $a^{-1} \equiv b^{-1}$, we know that $a \equiv b$, and thus the inverse of x is unique up to p.

We now have enough information to prove that $(p-2)! \equiv 1$. For $p > 2$, the key here is that every $p-i$ in $(p-2)! = (p-2)(p-3)\cdots(3)(2)$ has exactly one unique inverse, which is different from $p-i$. That means that we can split up this product into pairs of elements that are inverses of each other. Since each of these pairs multiplies to 1, by the definition of the inverse, the whole product is simply $(p-2)! \equiv 1$. Note that since $p > 2$, we know that p is odd, and thus there will be an even number of terms in $(p-2)(p-3)\cdots(3)(2)$. For $p = 2$, the special case, simply note that $p - 2 = 0$, and thus that $(p-2)! = 0! = 1$. Thus for all p, $(p-2)! \equiv 1$.

Now, since we know that $p - 1 \equiv -1$ and $(p-2)! \equiv 1$, it is clear that

$$(p-1)(p-2)! = (p-1)! \equiv -1 \cdot 1 = -1$$

Thus the claim is proved. ■

5. Solve each of the following for x.

`i)` $432x \equiv 2 \pmod{91}$

□ Note that $432 \equiv 68 \pmod{91}$. We first use the matrix layout algorithm to find $[68]^{-1}$:

$$\left(\begin{array}{cc|c} 1 & 0 & 68 \\ 0 & 1 & 91 \end{array}\right) \xrightarrow{r_2=r_2-r_1} \left(\begin{array}{cc|c} 1 & 0 & 68 \\ -2 & 1 & 23 \end{array}\right) \xrightarrow{r_1=r_1-2r_2}$$

$$\left(\begin{array}{cc|c} 3 & -2 & 22 \\ -1 & 1 & 23 \end{array}\right) \xrightarrow{r_2=r_2-r_1} \left(\begin{array}{cc|c} 3 & -2 & 22 \\ -4 & 3 & 1 \end{array}\right) \xrightarrow{r_1=r_1-22r_2}$$

$$\left(\begin{array}{cc|c} 91 & -68 & 0 \\ \mathbf{-4} & \mathbf{3} & \mathbf{1} \end{array}\right)$$

Thus we have

$$\begin{aligned} 1 &= 68 \cdot (-4) + 91 \cdot 3 \\ 1 \bmod 91 &= \big(68 \cdot (-4) + 91 \cdot 3\big) \bmod 91 \\ 1 \bmod 91 &= \big(68 \cdot (-4)\big) \bmod 91 + \big(91 \cdot 3\big) \bmod 91 \\ 1 &\equiv 68 \cdot (-4) \pmod{91} \end{aligned}$$

This implies that $[68]^{-1} = [-4]$. We now verify the conditions necessary to solve the equation. If $d = \gcd(432, 91)$, then it is true that $d = 1$. It is also true that $d | b$, since $1 | 2$. We then find $[x]$ as follows:

$$\begin{aligned} 432x &\equiv 2 \pmod{91} \\ 432^{-1} \cdot 432x &\equiv 432^{-1} \cdot 2 \pmod{91} \\ x &\equiv (-4) \cdot 2 \pmod{91} \\ x &\equiv -8 \equiv 83 \pmod{91} \end{aligned}$$

Thus $[x] = [83]$. ■

`ii)` $23x \equiv 16 \pmod{107}$
$\square$ We first use the matrix layout algorithm to find $[23]^{-1}$:

$$\left(\begin{array}{cc|c} 1 & 0 & 23 \\ 0 & 1 & 107 \end{array}\right) \xrightarrow{r_2=r_2-4r_1} \left(\begin{array}{cc|c} 1 & 0 & 23 \\ -4 & 1 & 15 \end{array}\right) \xrightarrow{r_1=r_1-r_2}$$
$$\left(\begin{array}{cc|c} 5 & -1 & 8 \\ -4 & 1 & 15 \end{array}\right) \xrightarrow{r_2=r_2-r_1} \left(\begin{array}{cc|c} 5 & -1 & 8 \\ -9 & 2 & 7 \end{array}\right) \xrightarrow{r_1=r_1-r_2}$$
$$\left(\begin{array}{cc|c} 14 & -3 & 1 \\ -9 & 2 & 7 \end{array}\right) \xrightarrow{r_2=r_2-7r_1} \left(\begin{array}{cc|c} \mathbf{14} & \mathbf{-3} & \mathbf{1} \\ -107 & 23 & 0 \end{array}\right)$$

Thus we have

$$\begin{aligned} 1 &= 23 \cdot 14 + 107 \cdot (-3) \\ 1 \bmod 107 &= \big(23 \cdot 14 + 107 \cdot (-3)\big) \bmod 107 \\ 1 \bmod 107 &= \big(23 \cdot 14\big) \bmod 107 + \big(107 \cdot (-3)\big) \bmod 107 \\ 1 &\equiv 23 \cdot 14 \pmod{107} \end{aligned}$$

This implies that $[23]^{-1} = [14]$. We now verify the conditions necessary to solve the equation. If $d = \gcd(23, 107)$, then it is true that $d = 1$. It is also true that $d \mid b$, since $1 \mid 16$. We then find $[x]$ as follows:

$$\begin{aligned} 23x &\equiv 16 \pmod{107} \\ 23^{-1} \cdot 23x &\equiv 432^{-1} \cdot 16 \pmod{107} \\ x &\equiv 14 \cdot 16 \pmod{107} \\ x &\equiv 224 \equiv 10 \pmod{107} \end{aligned}$$

Thus $[x] = [10]$. ■