Math 55—Fall 2025—Haiman
Homework 5

Problems from Rosen

Section 4.3

42. Use the extended Euclidean algorithm to express $\gcd(252, 356)$ as a linear combination of 252 and 356.

Answer: First, we apply the Euclidean algorithm to find the gcd:

$$\begin{aligned} 356 &= 1 \cdot 252 + 104 \\ 252 &= 2 \cdot 104 + 44 \\ 104 &= 2 \cdot 44 + 16 \\ 44 &= 2 \cdot 16 + 12 \\ 16 &= 1 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0 \end{aligned}$$

The last non-zero remainder is 4*, so* $\gcd(252, 356) = 4$.

Next, we use back-substitution to express 4 *as a linear combination of* 252 *and* 356*:*

$$\begin{aligned} 4 &= 16 - 1 \cdot 12 \\ &= 16 - 1 \cdot (44 - 2 \cdot 16) && \textit{Substitute } 12 = 44 - 2 \cdot 16 \\ &= 16 - 44 + 2 \cdot 16 = 3 \cdot 16 - 44 \\ &= 3(104 - 2 \cdot 44) - 44 && \textit{Substitute } 16 = 104 - 2 \cdot 44 \\ &= 3 \cdot 104 - 6 \cdot 44 - 44 = 3 \cdot 104 - 7 \cdot 44 \\ &= 3 \cdot 104 - 7(252 - 2 \cdot 104) && \textit{Substitute } 44 = 252 - 2 \cdot 104 \\ &= 3 \cdot 104 - 7 \cdot 252 + 14 \cdot 104 = 17 \cdot 104 - 7 \cdot 252 \\ &= 17(356 - 1 \cdot 252) - 7 \cdot 252 && \textit{Substitute } 104 = 356 - 1 \cdot 252 \\ &= 17 \cdot 356 - 17 \cdot 252 - 7 \cdot 252 = 17 \cdot 356 - 24 \cdot 252. \end{aligned}$$

Hence, $\gcd(252, 356) = 4 = (-24) \cdot 252 + 17 \cdot 356$.

46(e). Find the smallest positive integer with exactly 10 different positive factors.

Answer: The number of positive divisors of an integer n *with prime factorization* $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ *is given by* $\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$*. We need* $\tau(n) = 10$*. The ways to factor* 10 *are* 10 *and* $5 \cdot 2$*. This leads to two cases for the exponents:*

- ***Case 1:*** $a_1 + 1 = 10 \implies a_1 = 9$*. To minimize* $n = p_1^9$*, we choose the smallest prime,* $p_1 = 2$*. This gives* $n = 2^9 = 512$.
- ***Case 2:*** $(a_1 + 1)(a_2 + 1) = 5 \cdot 2 \implies a_1 = 4$ *and* $a_2 = 1$*. To minimize* $n = p_1^4 p_2^1$*, we assign the larger exponent to the smaller prime. Thus, we choose* $p_1 = 2$ *and* $p_2 = 3$*, which gives* $n = 2^4 \cdot 3^1 = 16 \cdot 3 = 48$.

Comparing the two cases, $48 < 512$*. The smallest such integer is* $\boxed{48}$.

54. Adapt Euclid's proof to show there are infinitely many primes of the form $3k + 2$.

Answer: We prove this by contradiction.

1. *Assume there are only a finite number of primes of the form* $3k + 2$*. Let this finite list of primes be* $p_1, p_2, \ldots, p_r$.
2. *Let* $N = 3(p_1 p_2 \cdots p_r) - 1$.
3. *We consider the prime factorization of* N*. Notice that* $N \equiv -1 \equiv 2 \pmod 3$*. This implies that* 3 *is not a prime factor of* N*.*

4. *Furthermore, for any prime p_i in our list, $N \equiv -1 \pmod{p_i}$. This means that none of the primes p_i divides N.*
5. *Since $N > 1$, it must have at least one prime factor. All prime factors of N must be of the form $3k+1$ or $3k+2$. They cannot all be of the form $3k+1$, because the product of numbers of the form $3k+1$ is itself of the form $3k+1$. (For example, $(3k_1+1)(3k_2+1) = 3(3k_1k_2+k_1+k_2)+1 \equiv 1 \pmod 3$.)*
6. *Since $N \equiv 2 \pmod 3$, at least one of its prime factors, let's call it q, must be of the form $3k+2$.*
7. *This prime q is of the form $3k+2$, but q cannot be in our original list $\{p_1, \dots, p_r\}$, since none of those primes divide N. This contradicts our assumption that our list contained all primes of the form $3k+2$.*

Thus, the assumption must be false, and there are infinitely many primes of the form $3k+2$.

Section 4.4

6(b). Find an inverse of a modulo m for $a = 34$, $m = 89$.

Answer: We use the extended Euclidean algorithm. First, the division steps:

$$\begin{aligned}
89 &= 2 \cdot 34 + 21\\
34 &= 1 \cdot 21 + 13\\
21 &= 1 \cdot 13 + 8\\
13 &= 1 \cdot 8 + 5\\
8 &= 1 \cdot 5 + 3\\
5 &= 1 \cdot 3 + 2\\
3 &= 1 \cdot 2 + 1
\end{aligned}$$

Now, we perform back-substitution to write 1 as a linear combination of 34 and 89:

$$\begin{aligned}
1 &= 3 - 1 \cdot 2\\
&= 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5\\
&= 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 = 2 \cdot 8 - 3 \cdot 5\\
&= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) = 5 \cdot 8 - 3 \cdot 13\\
&= 5 \cdot (21 - 1 \cdot 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13\\
&= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21) = 13 \cdot 21 - 8 \cdot 34\\
&= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 26 \cdot 34 - 8 \cdot 34\\
&= 13 \cdot 89 - 34 \cdot 34.
\end{aligned}$$

From $1 = 13 \cdot 89 - 34 \cdot 34$, we see that $1 \equiv (-34) \cdot 34 \pmod{89}$. So, the inverse of 34 is $-34 \equiv -34 + 89 \equiv \boxed{55} \pmod{89}$.

12(a). Solve the congruence $34x \equiv 77 \pmod{89}$ using the inverse from 6(b).

Answer: From 6(b), the inverse of 34 modulo 89 is 55. We multiply both sides of the congruence by 55:

$$x \equiv 55 \cdot 77 \pmod{89}.$$

To simplify the calculation, note that $77 \equiv -12 \pmod{89}$.

$$x \equiv 55 \cdot (-12) \equiv -660 \pmod{89}.$$

To find the value of $-660 \pmod{89}$, we can add multiples of 89: $-660 + 8 \cdot 89 = -660 + 712 = 52$. So, $x \equiv \boxed{52} \pmod{89}$.

16. (a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers that are inverses of each other modulo 11.

Answer: We need to find pairs (a, b) *from* $\{2, 3, 4, 5, 6, 7, 8, 9\}$ *such that* $ab \equiv 1 \pmod{11}$. *The pairs are:*

$$(2, 6) \text{ since } 2 \cdot 6 = 12 \equiv 1 \pmod{11},$$
$$(3, 4) \text{ since } 3 \cdot 4 = 12 \equiv 1 \pmod{11},$$
$$(5, 9) \text{ since } 5 \cdot 9 = 45 = 4 \cdot 11 + 1 \equiv 1 \pmod{11},$$
$$(7, 8) \text{ since } 7 \cdot 8 = 56 = 5 \cdot 11 + 1 \equiv 1 \pmod{11}.$$

These four pairs include all integers from 2 *to* 9.

(b) Use part (a) to show that $10! \equiv -1 \pmod{11}$.

Answer: We can write out $10!$ *and group the pairs of inverses:*

$$\begin{aligned} 10! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &\equiv 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \pmod{11} \\ &\equiv 1 \cdot (1) \cdot (1) \cdot (1) \cdot (1) \cdot 10 \pmod{11} \\ &\equiv 10 \pmod{11} \\ &\equiv \boxed{-1} \pmod{11}. \end{aligned}$$

Additional problems

1. By Bézout's theorem, given any $a, b \in \mathbb{Z}^+$, there are integers r, s such that $\gcd(a, b) = ra + sb$. Prove that if (r_0, s_0) is one such pair, then any other pair (r, s) must be of the form $(r, s) = \left(r_0 - k\frac{b}{g}, s_0 + k\frac{a}{g}\right)$ for some integer k, where $g = \gcd(a, b)$.

   Answer: Let $g = \gcd(a, b)$, and suppose (r_0, s_0) is a particular solution to $r_0a + s_0b = g$. Let (r, s) be any other solution, so $ra + sb = g$. Subtracting the first equation from the second gives:

   $$(r - r_0)a + (s - s_0)b = 0 \implies (r - r_0)a = -(s - s_0)b.$$

   Let $a = ga_0$ and $b = gb_0$, where $\gcd(a_0, b_0) = 1$. Substituting these into the equation gives:

   $$(r - r_0)ga_0 = -(s - s_0)gb_0 \implies (r - r_0)a_0 = -(s - s_0)b_0.$$

   This shows that a_0 divides the product $(s - s_0)b_0$. Since $\gcd(a_0, b_0) = 1$, by Euclid's Lemma, we must have $a_0 \mid (s - s_0)$. Therefore, $s - s_0 = ka_0$ for some integer k. Substituting this back into the equation $(r - r_0)a_0 = -(s - s_0)b_0$:

   $$(r - r_0)a_0 = -(ka_0)b_0 \implies r - r_0 = -kb_0.$$

   So, we have found that any other solution (r, s) must satisfy:

   $$s = s_0 + ka_0 = s_0 + k\frac{a}{g} \quad \textit{and} \quad r = r_0 - kb_0 = r_0 - k\frac{b}{g}.$$

   Conversely, any pair of this form is a valid solution, because:

   $$\left(r_0 - k\frac{b}{g}\right)a + \left(s_0 + k\frac{a}{g}\right)b = (r_0a + s_0b) - k\frac{ab}{g} + k\frac{ab}{g} = g.$$

   Thus, all solutions are of the specified form. $\square$

2. Prove that for all $a, b \in \mathbb{Z}^+$, the set of common divisors of a and b equals the set of divisors of $\gcd(a, b)$.

   Answer: We need to prove that for any integer d, $(d \mid a$ and $d \mid b) \iff d \mid \gcd(a, b)$.

   ($\Rightarrow$) *Let d be a common divisor of a and b. Let $g = \gcd(a, b)$. By Bézout's theorem, there exist integers r, s such that $g = ra + sb$. Since $d \mid a$ and $d \mid b$, d must divide any linear combination of a and b. Thus, $d \mid (ra + sb)$, which means $d \mid g$.*

   ($\Leftarrow$) *Let d be a divisor of $g = \gcd(a, b)$. By the definition of the greatest common divisor, we know that $g \mid a$ and $g \mid b$. Since $d \mid g$ and $g \mid a$, by the transitivity of divisibility, we have $d \mid a$. Similarly, since $d \mid g$ and $g \mid b$, we have $d \mid b$. Thus d is a common divisor of a and b.*

   This proves the two sets of divisors are identical. $\square$

3. Solve linear congruences $ax \equiv b \pmod{m}$ when a and m are not necessarily coprime.

   (a) Let $g = \gcd(a, m)$. Show that if $g \nmid b$, then $ax \equiv b \pmod{m}$ has no solution.

   Answer: The congruence $ax \equiv b \pmod{m}$ is equivalent to the equation $ax - b = km$ for some integer k. This can be rewritten as $ax - km = b$. Let $g = \gcd(a, m)$. By definition, $g \mid a$ and $g \mid m$. Therefore, g must divide any integer linear combination of a and m, which includes $ax - km$. So, $g \mid b$. This shows that if a solution exists, it is necessary that g divides b. Therefore, by contraposition, if $g \nmid b$, then the congruence has no solution. $\square$

   (b) If $g \mid b$, set $a' = a/g$, $b' = b/g$, $m' = m/g$. Show $\gcd(a', m') = 1$ and that $ax \equiv b \pmod{m}$ has the same solutions as $a'x \equiv b' \pmod{m'}$.

   Answer: First, we show $\gcd(a', m') = 1$. Since $g = \gcd(a, m)$, we can write $a = ga'$ and $m = gm'$. Suppose $d = \gcd(a', m')$. Then $d \mid a'$ and $d \mid m'$, which implies that $dg \mid ga'$ and $dg \mid gm'$. Thus, dg is a common divisor of a and m. Because g is the greatest *common* *divisor, we must have $dg \leq g$. Since $g > 0$, this implies $d \leq 1$. As a gcd, d must be positive, so $d = 1$.*

Next, we show the congruences are equivalent. The congruence $ax \equiv b \pmod{m}$ is equivalent to the equation $ax - b = km$ for some integer k. Since $g \mid a$, $g \mid b$, and $g \mid m$, we can divide the entire equation by g:

$$\frac{a}{g}x - \frac{b}{g} = k\frac{m}{g} \iff a'x - b' = km'$$

This new equation is precisely the definition of the congruence $a'x \equiv b' \pmod{m'}$. Since the step of dividing or multiplying by the non-zero integer g is reversible, the two congruences have the exact same set of integer solutions for x. □

(c) Use (b) to solve $28x \equiv 12 \pmod{40}$ and list all solutions modulo 40.

Answer: Here, $a = 28$, $b = 12$, and $m = 40$. First, we find $g = \gcd(28, 40) = 4$. Since $g = 4$ and $4 \mid 12$, solutions exist. We reduce the congruence using the results from part (b):

$$a' = 28/4 = 7, \quad b' = 12/4 = 3, \quad m' = 40/4 = 10.$$

The equivalent congruence is $7x \equiv 3 \pmod{10}$. To solve this, we find the inverse of 7 modulo 10. By inspection, $7 \cdot 3 = 21 \equiv 1 \pmod{10}$, so $7^{-1} \equiv 3 \pmod{10}$. Multiplying the congruence by 3:

$$x \equiv 3 \cdot 3 \equiv 9 \pmod{10}.$$

This means the solutions are of the form $x = 9 + 10k$ for any integer k. We want the solutions in the range $[0, 39]$.

* $k = 0 : x = 9$
* $k = 1 : x = 19$
* $k = 2 : x = 29$
* $k = 3 : x = 39$

There are $g = 4$ incongruent solutions modulo 40. The set of solutions is $\boxed{\{9, 19, 29, 39\}}$.