► **Problem 4.2-12(g)(j)** In each of the following cases, find the greatest common divisor of a and b and express it in the form $ma + nb$ for suitable integers m and n.

(g) $a = -3719$ and $b = 8416$.

(j) $a = 12345$ and $b = 54321$.

Solution. (g)

8416	1	0
3719	0	1
978	1	-2
785	-3	7
193	4	-9
13	-19	43
11	270	-611
2	-289	654
1	1715	-3881

The last nonzero remainder is 1, so $\gcd(8416, 3719) = 1 = (1715) \times (8461) + (-3881) \times (3719)$. Thus, $\gcd(-3719, 8416) = 1 = (3881) \times (-3719) + (1715) \times (8461)$.

(j)

54321	1	0
12345	0	1
4941	1	-4
2463	-2	9
15	5	-22
3	-822	3617

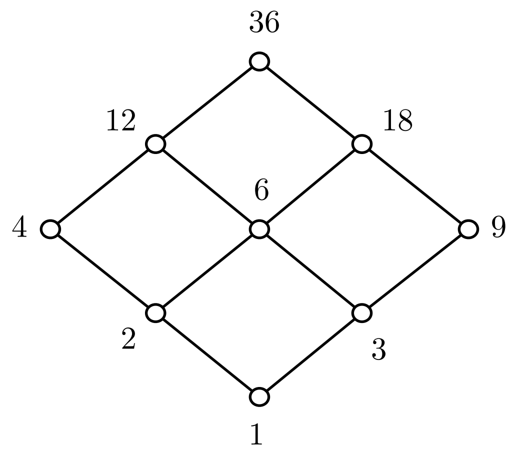
Since the last nonzero remainder is 3, $\gcd(12345, 54321) = 3 = (-822) \times (54321) + (3617) \times (12345)$. □

▶ **Problem 4.2-20** If $k \in \mathbf{N}$, prove that $\gcd(3k+2, 5k+3) = 1$.

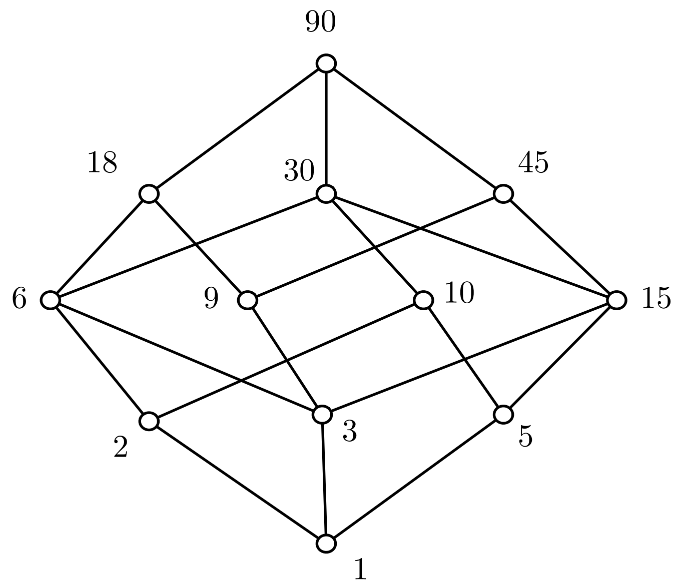
Proof. Let x be the greatest common divisor of $3k+2$ and $5k+3$ for any $k \in \mathbf{N}$. Then, $x|3k+2$ and $x|5k+3$. Clearly, $x|5(3k+2)$ and $x|3(5k+3)$, and it further implies $x|[5(3k+2) - 3(5k+3)]$. Thus $x|1$. From the fact that 1 can be divides by an integer x, we have $x = 1$, and so $\gcd(3k+2, 5k+3) = 1$. $\square$

► **Problem 4.2-35(c)(d)** Let n be a natural number, $n > 1$. Let $A = \{a \in \mathbf{N} \mid a|n\}$. Draw the Hasse diagram associated with the poset $(A, |)$ for $n = 36$ and $n = 90$.

Solution. (c)



(d)



□

▶ **Problem 4.3-18(b)(c)**

(b) Is $2^{91}-1$ prime? Explain your answer.

(c) Show that if 2^n-1 is prime then necessarily n is prime.

Solution.

(b) No, because $2^{91}-1=(2^{13}-1)(2^{78}+2^{65}+2^{52}+2^{39}+2^{26}+2^{13}+1)$.

(c) If n is not a prime, we write $n=rs$ for $1<r,s<n$. Then $2^n-1=2^{rs}-1=(2^r-1)(2^{r(s-1)}+2^{r(s-2)}+\cdots+2^r+1)$ is not a prime, a contradiction. □

► **Problem 4.3-35** Let a, b, and c be integers each relatively prime to another integer n. Prove that the product abc is relatively prime to n.

Proof. If abc and n are not relatively prime, then there exists a prime p such that $p|abc$ and $p|n$. By Corollary 4.3.8, $p|a$ or $p|b|$ or $p|c$. In the first case, $p|a$ and $p|n$ contradict $\gcd(a, n) = 1$. The other two cases are similar. □

► **Problem 4.3-32(b)(c)** Let a and b be integers. Let p be a prime. Answer true or false and explain:
(b) If $p|a$ and $p|(a^2 + b^2)$, then $p|b$.
(c) If $p|(a^9 + a^{17})$, then $p|a$.

Solution. (b) True. Since $p|a$, it implies $p|a^2$. Now, $p|a^2$ and $p|(a^2 + b^2)$ forces $p|b^2$. Then, by Proposition 4.3.7, we conclude that $p|b$.

(c) False. Consider $p = 257$ and $a = 2$. Clearly, p is a prime. Then $2^9 + 2^{17} = 131584$ and $257|(2^9 + 2^{17})$. However, $257 \nmid 2$. □

▶ **Problem 4.3-35**

Suppose p and $p+2$ are twin primes and $p > 3$. Prove that $6|(p+1)$.

Proof. Since p and $p+2$ are primes and $p > 3$, it implies that $p+1$ is an even integer, i.e., $2|(p+1)$. Also, we have known that there is a multiple of 3 in any three consecutive positive integers p, $p+1$ and $p+2$. Again, by the fact that p and $p+2$ are primes, it must be $3|(p+1)$. Therefore, we have $6|(p+1)$. □

Another Proof. Write $p+1 = 6q + r$ with $0 \leqslant r < 6$ for some integer q. Consider the following cases.

If $r = 1$, then $p = 6q$, contradicting that p is a prime.

If $r = 2$, then $p = 6q + 1$, so $p + 2 = 6q + 3$. Thus, $3|(p+2)$, contradicting that $p+2$ is a prime.

If $r = 3$, then $p = 6q + 2$ is divisible by 2, contradicting that p is a prime.

If $r = 4$, then $p = 6q + 3$ is divisible by 3, contradicting that p is a prime.

If $r = 5$, then $p = 6q + 4$ is divisible by 2, contradicting that p is a prime.

Therefore, the only possibility is that $r = 0$, that is, $6|(p+1)$. □

► **Problem 4.4-9(i)(j)** Find all integers x, $0 \leqslant x < n$, satisfying each of the following congruences mod n. If no such x exists, explain why not.
(b) $65x \equiv 27 \pmod{n}$, $n = 169$.
(c) $4x \equiv 320 \pmod{n}$, $n = 592$.

Solution. (i) No x exists. If $65x \equiv 27 \pmod{169}$, then $169|(65x - 27)$, so $13|(65x - 27)$. Since $13|65x$, it implies $13|27$, a contradiction.

(j) If $4x \equiv 320 \pmod{592}$, then $4x = 320+592k$ for some $k \in \mathbf{Z}$. That is, $x = 80+148k$. The value of x are 80, 288, 376, 524. $\square$

▶ **Problem 4.4-10** Given integer a, b, c, d, x and a prime p, suppose $(ax+b)(cx+d) \equiv 0 \pmod{p}$. Prove that $ax + b \equiv 0 \pmod{p}$ or $cx + d \equiv 0 \pmod{p}$.

Proof. $(ax + b)(cx + d) \equiv 0 \pmod{p}$ implies $P|(ax + b)(cx + d)$. Since p is prime, by Proposition 4.3.7, we conclude that $p|(ax + b)$ or $p|(cx + d)$. The first case says that $ax + b \equiv 0 \pmod{p}$ and the second that $cx + d \equiv 0 \pmod{p}$, given the desired result. □

► **Problem 4.4-11(d)**

Find all integers x and y, $0 \leqslant x, y < n$, that satisfy each of the following pair of congruences. If no x, y exist, explain why not.

$$\begin{cases} 7x + 2y \equiv 3 \pmod{n} & n = 15 \\ 9x + 4y \equiv 6 \pmod{n} \end{cases}$$

Solution. Multiply the first congruence by 2 to get $14x + 4y \equiv 6 \pmod{15}$. Subtracting the second congruence gives $5x \equiv 0 \pmod{15}$, so $x = 0, 3, 6, 9$ or 12.

If $x = 0$, then $2y \equiv 3 \pmod{15}$, and so $y = 9$.

If $x = 3$, then $2y \equiv 3 - 21 = -18 \equiv 12 \pmod{15}$, and so $y = 6$.

If $x = 6$, then $2y \equiv 3 - 42 = -39 \equiv 6 \pmod{15}$, and so $y = 3$.

If $x = 9$, then $2y \equiv 3 - 63 = -60 \equiv 0 \pmod{15}$, and so $y = 0$.

If $x = 12$, then $2y \equiv 3 - 84 = -81 \equiv 9 \pmod{15}$, and so $y = 12$. □

▶ **Problem 4.4-11(e)**

Find all integers x and y, $0 \leqslant x, y < n$, that satisfy each of the following pair of congruences. If no x, y exist, explain why not.

$$\begin{cases} 3x + 5y \equiv 14 \pmod{n} & n = 28 \\ 5x + 9y \equiv 6 \pmod{n} \end{cases}$$

Solution. Multiply the first congruence by 5 and the second by 3 gives

$$\begin{cases} 15x + 25y \equiv 70 \equiv 14 \pmod{28} \\ 15x + 27y \equiv 18 \pmod{28}. \end{cases}$$

Subtracting the first congruence from the second gives $2y \equiv 4 \pmod{28}$. Thus, $y = 2$ or $y = 16$.

If $y = 2$, then $3x \equiv 14 - 10 = 4 \pmod{28}$, and so $x = 20$.

If $y = 16$, then $3x \equiv 14 - 80 = -66 \equiv 18 \pmod{28}$, and so $x = 6$. □

▶ **Problem 4.4-16** Prove that an integer $(a_{n-1}a_{n-2}\cdots a_0)_{10}$ is divisible by 11 if and only if $a_0 + a_2 + a_4 + \cdots \equiv a_1 + a_3 + a_5 + \cdots \pmod{11}$. [Hint: $10 \equiv -1 \pmod{11}$.]

Proof. From the hint $10 \equiv -1 \pmod{11}$ and Proposition 4.4.7, we note that

$$10^k \equiv (-1)^k \pmod{11}$$

for any natural number k. Since

$$(a_{n-1}a_{n-2}\cdots a_2a_1a_0)_{10} = a_{n-1}\cdot 10^{n-1} + a_{n-2}\cdot 10^{n-2} + \cdots + a_3\cdot 10^3 + a_2\cdot 10^2 + a_1\cdot 10 + a_0$$

we have

$$\begin{aligned} & (a_{n-1}a_{n-2}\cdots a_2a_1a_0)_{10} \\ \equiv\ & a_{n-1}\cdot(-1)^{n-1} + a_{n-2}\cdot(-1)^{n-2} + \cdots - a_3 + a_2 - a_1 + a_0 \pmod{11}. \end{aligned}$$

and this is 0 (mod 11) if and only if $a_0 + a_2 + a_4 + \cdots \equiv a_1 + a_3 + a_5 + \cdots \pmod{11}$. $\square$

▶ **Problem 4.5-15** Does the test in (7) detect transposition errors: that is, will it notice if two (different) adjacent digits have ben interchange? Explain.

The check digit for Universal Product Codes is determined by the rule:

(7) 3(sum of digits in odd positions)+(sum of digits in even positions)$\equiv 0 \pmod{10}$.

Solution. Suppose that $a_1–a_2a_3a_4a_5a_6–a_7a_8a_9a_{10}a_{11}–x$ is a valid universal product code. Thus,

$$A = 3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + (a_2 + a_4 + a_6 + a_8 + a_{10} + x) \equiv 0 \pmod{10}$$

If a_2 and a_3 are transposed, the error will not be detected provided

$$B = 3(a_1 + a_2 + a_5 + a_7 + a_9 + a_{11}) + (a_3 + a_4 + a_6 + a_8 + a_{10} + x) \equiv 0 \pmod{10}$$

Now $A - B = 3(a_3 - a_2) + (a_2 - a_3) = 2(a_3 - a_2)$. So, if $a_3 - a_2 = 5$, we'll have $A - B \equiv 0 \pmod{10}$. Hence, $B \equiv A \equiv 0 \pmod{10}$ and the transposition will not be detected. We conclude that the test given by (7) does **not** detect errors due to the transposition of adjacent digits. □

▶ **Problem 4.5-18** Find the smallest nonnegative integer x that satisfies the given system of congruences.

$x \equiv 1 \pmod{4}$

$x \equiv 8 \pmod{9}$

$x \equiv 10 \pmod{25}$

Solution. We first solve $x \equiv 1 \pmod{4}$ and $x \equiv 8 \pmod{9}$.

Since $1 = 1 \cdot 9 + (-2) \cdot 4$, we have $x = 1 \cdot 1 \cdot 9 + (-2) \cdot 8 \cdot 4 = -55 \equiv 17 \pmod{36}$.

Then we solve $x \equiv 10 \pmod{25}$ and $x \equiv 17 \pmod{36}$.

Since $1 = 13 \cdot 25 + (-9) \cdot 36$, we have $x = 13 \cdot 17 \cdot 25 + (-9) \cdot 10 \cdot 36 = 2285 \equiv 485 \pmod{900}$.

Therefore, $x = 485$. $\square$

▶ **Problem 4.5-21(b)** Find a positive integer x such that $ab \equiv x$ modulo a suitable integer. Assuming that $ab < 50000$, find ab itself, if possible, and explain your reasoning.
$a \equiv 7$, $b \equiv 7 \pmod{8}$
$a \equiv 9$, $b \equiv 8 \pmod{27}$
$a \equiv 29$, $b \equiv 18 \pmod{125}$

Solution.

$ab \equiv 7 \cdot 7 \equiv 1 \pmod{8}$
$ab \equiv 9 \cdot 8 \equiv 18 \pmod{27}$
$ab \equiv 29 \cdot 18 \equiv 22 \pmod{125}$

We first solve $ab \equiv 1 \pmod{8}$ and $ab \equiv 18 \pmod{27}$
Since $1 = 3 \cdot 27 + (-10) \cdot 8$, we obtain
$ab \equiv 1 \cdot 3 \cdot 27 + 18 \cdot (-10) \cdot 8 = -1359 \equiv 153 \pmod{216}$.

Then, we solve $ab \equiv 22 \pmod{125}$ and $ab \equiv 153 \pmod{216}$.
Since $1 = (-19) \cdot 125 + 11 \cdot 216$, we obtain
$ab \equiv 153 \cdot (-19) \cdot 125 + 22 \cdot 11 \cdot 216 = -311103 \equiv 12897 \pmod{27000}$.
Since $ab < 50000$, we have $x = 12897$ or $x = 39897$. $\square$

▶ **Problem 4.5-21(c)** Find a positive integer x such that $ab \equiv x$ modulo a suitable integer. Assuming that $ab < 50000$, find ab itself, if possible, and explain your reasoning.
$a \equiv 1$, $b \equiv 2 \pmod 8$
$a \equiv 8$, $b \equiv 1 \pmod{27}$
$a \equiv 55$, $b \equiv 82 \pmod{125}$

Solution.

$ab \equiv 1 \cdot 2 \equiv 2 \pmod 8$
$ab \equiv 8 \cdot 1 \equiv 8 \pmod{27}$
$ab \equiv 55 \cdot 82 \equiv 10 \pmod{125}$

We first solve $ab \equiv 2 \pmod 8$ and $ab \equiv 8 \pmod{27}$
Since $1 = 3 \cdot 27 + (-10) \cdot 8$, we obtain
$ab \equiv 2 \cdot 3 \cdot 27 + 8 \cdot (-10) \cdot 8 = -478 \equiv 170 \pmod{216}$.

Then, we solve $ab \equiv 10 \pmod{125}$ and $ab \equiv 170 \pmod{216}$.
Since $1 = (-19) \cdot 125 + 11 \cdot 216$, we obtain
$ab \equiv 170 \cdot (-19) \cdot 125 + 10 \cdot 11 \cdot 216 = -379990 \equiv 25010 \pmod{27000}$.
Since $ab < 50000$, $x = 25010$ is the unique solution. $\square$

► **Problem 4.5-23(b)(d)(e)** Suppose $p = 17$, $q = 23$, and $s = 5$. How would you encode each of the following "messages"?

(b) **HELP**

(d) **BYE**

(e) **NOW**

Solution.

$$r = p \cdot q = 17 \times 23 = 391.$$

(b) **HELP** corresponds to the number 08051216.
Thus, $E = (8051216)^5 \pmod{391} = 33$.

(d) **BYE** corresponds to the number 022505.
Thus, $E = (22505)^5 \pmod{391} = 97$.

(e) **NOW** corresponds to the number 141523.
Thus, $E = (141523)^5 \pmod{391} = 104$. □

► **Problem 4.5-25(b)**

Suppose $p = 17$, $q = 59$, and $s = 3$. If you receive $E = 926$, what is the message?

Solution. We first note that $\gcd(3, 16) = 1$ and $11(3) + (-2)(16) = 1$, so $a = 11$. Also, $\gcd(3, 58) = 1$ and $39(3) + (-2)(58) = 1$, so $b = 39$. Then $E^a = 926^{11} \equiv 8^{11} = 8(8^2)^5 \equiv 8 \cdot 13^5 \equiv 2 \pmod{17}$, while $E^b = 926^{39} \equiv 41^{39} = 41(41^2)^{19} \equiv 41 \cdot 29^{19} = 41(29^3)(29^4)^4 \equiv 41 \cdot 22 \cdot 48^4 \equiv 41 \cdot 22 \cdot 3^2 = 8118 \equiv 35 \pmod{59}$. Thus,

$$E^a \equiv 2 \pmod{17}$$

$$E^a \equiv 35 \pmod{59}$$

Since $1 = 7(17) - 2(59)$, we have $E = 2 \cdot (-2) \cdot 59 + 35 \cdot 7 \cdot 17 = 3929 \equiv 920 \pmod{1003}$. The message is **IT**. $\square$