In Exercises 1 through 4, for the given integers m and n, write m as $qn + r$, with $0 \le r < n$.

1. $m = 20, n = 3$
2. $m = 64, n = 37$
3. $m = 3, n = 22$
4. $m = 48, n = 12$

1. $m = 3 \cdot 6 + 2$
2. $m = 1\ 37 + 27$
3. $m = 0\ 22 + 3$
4. $m = 4 \cdot 12 + 0$

5. Write each integer as a product of powers of primes (as in Theorem 3).

(a) 828 (b) 1666 (c) 1781
(d) 1125 (e) 107

(a) $828 = 2 \cdot 2 \cdot 3 \cdot 3\ 23$

(b) $1666 = 2 \cdot 7 \cdot 7 \cdot 3 \cdot 5$

(c) $1781 = 13 \cdot 13\ 137$

(d) $1125 = 5\ 5 \cdot 5 \cdot 3 \cdot 3$

(e) $107 = 107$

In Exercises 6 through 9, find the greatest common divisor d of the integers a and b, and write d as sa + tb.

6. $a = 60$, $b = 100$ **7.** $a = 45$, $b = 33$

8. $a = 34$, $b = 58$ **9.** $a = 77$, $b = 128$

6. $a = 100$, $b = 60$

$100 = 1 \cdot 60 + 40$

$60 = 1 \cdot 40 + 20$

$40 = 2 \cdot 20 + 0 \Rightarrow d = 20 = 60 - 40 = 60 - (100 - 60)$

$= \underline{(-1)} \cdot 100 + \underline{2} \cdot 60$

7. $a = 45$, $b = 33$

$45 = 1 \cdot 33 + 12$

$33 = 2 \cdot 12 + 9$

$12 = 1 \cdot 9 + 3$

$9 = 3 \cdot 3 + 0 \Rightarrow d = 3 = 12 - 9 = (45 - 33) - (33 - 2 \cdot 12)$

$= 45 - 2 \cdot 33 + 2 \cdot 12 = 45 - 2 \cdot 33 + 2 \cdot (45 - 33)$

$= 45 - 2 \cdot 33 + 2 \cdot 45 - 2 \cdot 33 = 3 \cdot 45 - 4 \cdot 33 =$

$\underline{3} \cdot 45 + \underline{(-4)} \cdot 33$

8. $a=34$, $b=58$

$a=58$, $b=34$

$58 = 1 \cdot 34 + 24$

$34 = 24 + 10$

$24 = 2 \cdot 10 + 4$

$10 = 2 \cdot 4 + 2$

$4 = 2 \cdot 2 + 0 \Rightarrow d = 2 = 10 + (-2) \cdot 4 =$

$= (34 - 24) + (-2)(24 - 2 \cdot 10) =$

$= [34 - (58 - 34)] + (-2) \cdot [(58 - 34) - 2 \cdot (34 - (58 - 34))]$

$= 2 \cdot 34 - 58 - 2(58 - 34 - 2(2 \cdot 34 - 58))$

$= 2 \cdot 34 - 58 - 2(58 - 34 - 4 \cdot 34 + 2 \cdot 58)$

$= 2 \cdot 34 - 58 - 2(3 \cdot 58 - 5 \cdot 34)$

$= (-7) \cdot 58 + 12 \cdot 34$

9) $a = 128, \ b = 77$

$128 = 1 \cdot 77 + 51$

$77 = 1 \cdot 51 + 26$

$51 = 1 \cdot 26 + 25$

$26 = 1 \cdot 25 + 1$

$25 = 25 \cdot 1 + 0 \Rightarrow d = 1 = 26 - 25$

$= 77 - 51 - (51 - 26)$

$= 77 - (128 - 77) - (128 - 77) + (77 - 51)$

$= 4 \cdot 77 - 2 \cdot 128 - 51$

$= 4 \cdot 77 - 2 \cdot 128 - (128 - 77)$

$= 5 \cdot 77 - 3 \cdot 128$

In Exercises 10 through 13, find the least common multiple of the integers.

10. 72, 108 **11.** 150, 70

12. 175, 245 **13.** 32, 27

10. $108 = 1 \cdot 72 + 36$

$72 = 2 \cdot 36 + 0 \Rightarrow d = 36$

$36 \cdot c = 2 \cdot 36 \cdot 3 \cdot 36 \Rightarrow c = 6 \; 36 = 216$

11. $150 = 2 \cdot 70 + 10$

$70 = 7 \cdot 10 + 0 \Rightarrow d = 10$

$10 \cdot c = 15 \cdot 10 \cdot 7 \; 10 \Rightarrow c = 15 \; 7 \; 10 = 1050$

12. $245 = 1 \; 175 + 70$

$175 = 2 \cdot 70 + 35$

$70 = 2 \cdot 35 + 0 \Rightarrow d = 35$

$35 \cdot c = 7 \; 35 \cdot 5 \cdot 35 \Rightarrow c = 5 \cdot 7 \; 35 =$

$$\begin{array}{r} 35 \cdot \\ 35 \\ \hline 175 \\ 105 \\ \hline \boxed{1225} \end{array}$$

13. $32 = 1 \; 27 + 5$

$27 = 5 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0 \Rightarrow d = 1$

$1 \cdot c = 32 \cdot 27 = 864$

$$\begin{array}{r} 32 \cdot \\ 27 \\ \hline 224 \\ 64 \\ \hline 864 \end{array}$$

14. If f is the mod-7 function, compute each of the following.

(a) $f(17)$ (b) $f(48)$ (c) $f(1207)$
(d) $f(130)$ (e) $f(93)$ (f) $f(169)$

(a) 3 ; (b) 6 ; (c) 3 ; (d) 4
(e) 2 , (f) 1

1207 | 7
7 | 172
=50
49
=17
14
=3

15. If g is the mod-6 function, solve each of the following.

(a) $g(n) = 3$ (b) $g(n) = 1$

(a) $n = 3$, (b) $n = 1$

16. Let a and b be integers. Prove that if p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. (*Hint:* If $p \nmid a$, then $1 = \text{GCD}(a, p)$; use Theorem 4 to write $1 = sa + tp$.)

Becouse p is prime $\Rightarrow$ 2 cases.

$\underline{\text{I}}$) If $p \nmid a \Rightarrow GCD(p, a) = 1$

$1 = \alpha p + \beta a \ / \cdot b \Leftrightarrow b = \alpha b p + \beta a b$

And $p \mid ab \Rightarrow p \mid \beta ab$
And $p \mid p \Rightarrow p \mid \alpha b p$ } $\Rightarrow p \mid \alpha b p + \beta a b = b \Rightarrow$

$p \mid b$

$\underline{\text{II}}$) If $p \nmid b \Rightarrow GCD(p, b) = 1.$

$1 = \alpha p + \beta b \ / \ a \Leftrightarrow a = \alpha a p + \beta a b$

And $p \mid ab \Rightarrow p \mid \beta ab$
And $p \mid p \Rightarrow p \mid \alpha a p$ } $\Rightarrow p \mid \alpha a p + \beta a b = b \Rightarrow$

$p \mid a$

From $\underline{\text{I}}$ & $\overline{\text{II}} \Rightarrow$ If p prime $\wedge$ $p \mid ab \Rightarrow$

$p \mid a \vee p \mid b$ ■

17. Show that if GCD$(a, c) = 1$ and $c \mid ab$, then $c \mid b$.

If $GCD(a,c)=1 \Rightarrow \alpha a + \beta c = 1 \;/\cdot b \Leftrightarrow$

$\alpha a b + \beta b c = b$

And becouse $c \mid ab \Rightarrow c \mid \alpha a b$

And becouse $c \mid c \Rightarrow c \mid \beta b c$ $\Big\} \Rightarrow$

$\Rightarrow c \mid \alpha a b + \beta b c \Leftrightarrow c \mid b$ $\blacksquare$

18. Show that if GCD$(a, c) = 1$, $a \mid m$, and $c \mid m$, then $ac \mid m$. (*Hint:* Use Exercise 17.)

$GCD(a,c) = 1 = \alpha a + \beta c \;/\cdot m \Rightarrow$

$m = \alpha a m + \beta c m = \alpha a c q_1 + \beta c a q_2$

$ac \mid \alpha a c q_1$

$ac \mid \beta c a q_2$ $\Big\} \Rightarrow ac \mid \alpha a c q_1 + \beta c a q_2 = m$ $\blacksquare$

19. Show that if $d = \mathrm{GCD}(a, b)$, $a \mid b$, and $c \mid d$, then $ac \mid bd$.

$\mathrm{GCD}(a, b) = d = \alpha a + \beta b$

$c \mid d \iff c \mid (\alpha a + \beta b)$

$a \mid b \Rightarrow b = q_1 a$

$c \mid (\alpha a + \beta q_1 a) = a(\alpha + \beta q_1) \Rightarrow c \mid a$

$a \mid b$ $\Rightarrow c \mid b$

$\mathrm{GBD}(a, b) = d = \alpha a + \beta b \; / \; b \Rightarrow bd = \alpha a b + \beta b^2$

$a \mid b \Rightarrow b = q_1 a$

$c \mid d \Rightarrow d = q_4 c$

$c \mid a \Rightarrow a = q_2 c$

$c \mid b \Rightarrow b = q_3 c$

$a \mid b \wedge c \mid b \Rightarrow ac \mid bb \wedge ac \mid ab$

$\Rightarrow ac \mid b^2 \Rightarrow ac \mid \beta b^2$ $\Rightarrow ac \mid \alpha a b + \beta b^2 = bd$ ∎

$\Rightarrow ac \mid \alpha a b$

20. Show that $\mathrm{GCD}(ca, cb) = c\,\mathrm{GCD}(a, b)$.

$\mathrm{GCD}(ca, cb) = \alpha ca + \beta cb = c(\alpha a + \beta b) = c\ \mathrm{GCD}(a, b)$ $\blacksquare$

21. Show that $\mathrm{LCM}(a, ab) = ab$.

$a \mid a \Rightarrow a \mid ab$
$ab \mid ab$
$\Rightarrow ab$ is a common multiple of a & ab $\Rightarrow$ $\mathrm{LCM}(a, ab) = ab$

(can't have something smaller then ab). $\blacksquare$

22. Show that if GCD$(a, b) = 1$, then LCM$(a, b) = ab$.

$$\mathrm{GCD}(a,b) \cdot \mathrm{LCM}(a,b) = ab \iff$$

$$1 \; \mathrm{LCM}(a,b) = ab \iff$$

$$\mathrm{LCM}(a,b) = ab \; \blacksquare$$

23. Let $c = \mathrm{LCM}(a, b)$. Show that if $a \mid k$ and $b \mid k$, then $c \mid k$.

$$\mathrm{GCD}(a,b) \; \mathrm{LCM}(a,b) = a \cdot b$$

$$\mathrm{GCD}(a,b) \cdot c = a \cdot b$$

$$(\alpha a + \beta b) \cdot c = a \cdot b \Rightarrow c \mid ab$$

$$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_n^{b_n}$$

$$K = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_n^{k_n}$$

$$a \mid K \Rightarrow a_i \leq k_i, \; (\forall) i \in \overline{1,n}$$

$$b \mid K \Rightarrow b_i \leq k_i, \; (\forall) i \in \overline{1,n}$$

$$\mathrm{LCM}(a,b) = c \Rightarrow c = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}, \; c_i = \max(a_i, b_i)$$

$$, i \in \overline{1,n}, \Rightarrow c_i \leq k_i, (\forall) i \in 1,n \iff c \mid K \; \blacksquare$$

24. Prove that if a and b are positive integers such that $a \mid b$ and $b \mid a$, then $a = b$.

$$a \mid b \Rightarrow b = q_1 a \,, \; q_1 \in \mathbb{Z}^+$$

$$b \mid a \Rightarrow a = q_2 b \,, \; q_2 \in \mathbb{Z}^+$$

$$b = q_1 q_2 b \Leftrightarrow 1 = q_1 q_2 \,; \; q_1, q_2 \in \mathbb{Z}^+$$

$$\Rightarrow q_1 = q_2 = 1 \Rightarrow$$

$$\left\{ \begin{array}{l} b = q_1 a = a \\ a = q_2 b = b \end{array} \right\} \Rightarrow a = b \quad \blacksquare$$

25. Let a be an integer and let p be a positive integer. Prove that if $p \mid a$, then $p = \text{GCD}(a, p)$.

$p \mid a$, $p \mid p$ $\Rightarrow$ p is a common divisor of a & p and is the greatest becouse if not $p + k \nmid p$, $(\forall) k > 0$ $\blacksquare$