NO: Divisibility Chapter 10.

DATE:

1. (i) $\gcd(17, 29)$

$29 = 1(17) + 12$

$17 = 1(12) + 5.$

$12 = 2(5) + 2$

$5 = 2(2) + 1$

$2 = 2(1) + 0$

$\underline{\gcd(17, 29) = 1}$

$1 = 5 - 2(2)$

$1 = 5 - 2(12 - 2(5))$

$1 = 5 - 2(12) + 4(5)$

$1 = 5(5) - 2(12)$

$1 = 5[17 - 12] - 2(12)$

$1 = 5(17) - 5(12) - 2(12)$

$1 = 5(17) - 7(12)$

$1 = 5(17) - 7(29 - 17)$

$1 = 12(17) - 7(29)$

For $d = sa + tb$

$s = 12,\ t = -7$

2(i) Note:

$ax + by = c$ has a solution

$\Leftrightarrow d | c$ where $d = \gcd(a, b)$.

If (x_0, y_0) is any particular Solution, all other solution are of the form

$x = x_0 + \left(\frac{b}{d}\right)u$

$y = y_0 - \left(\frac{a}{d}\right)u \quad ; u \in \mathbb{Z}$

Let $d = \gcd(a, b)$ and

$d = sa - tb \ ; \ s, t \in \mathbb{Z}^+$

consider $ax + by = 1$

2(i) $x = 12 + \left(\frac{29}{1}\right)u$

$y = -7 - (17)u$

$; u \in \mathbb{Z}$

we want $y = -t$, $t \in \mathbb{Z}$

so $y < 0$.

and $u \in \{0, 1, 2, \ldots\}$

(s, t):

$(12, 7), (41, 24),$

$(70, 41), \ldots$

NO:.......................... DATE:..........................

1 (ii) $\gcd(552, 713)$

$713 = 1(552) + 161$

$552 = 3(161) + 69$

$161 = 2(69) + 23.$

$69 = 3(23) + 0$

$\gcd(552, 713) = 23.$

$23 = 161 - 2(69)$

$23 = 161 - 2(552 - 3(161))$

$= 161 - 2(552) + 6(161)$

$= 7(161) - 2(552)$

$= 7(713 - 552) - 2(552)$

$= 7(713) - 9(552)$

2 (ii) For $d = \gcd(713, 552)$

and $23 = s(713) - t(552)$ — ①

let $x_0 = 7$ and $y_0 = -9$

we want $s, t \in \mathbb{Z}^+$

$x = 7 + (\frac{552}{23})u$

$x = 7 + 24u$ and

$y = -9 - (\frac{713}{23})u$

$y = -9 - 31u.$

For t in ① to be positive we need the y in $ax + by = c$ to be negative

$-9 - 31u < 0$ for $u \in \{0, 1, 2, \ldots\}$

(s,t): $(7, 9)$, $(31, 40)$ $(55, 71), \ldots$

1 (iii) $\gcd(299, 345)$

$345 = 1(299) + 46$

$299 = 6(46) + 23$

$46 = 2(23) + 0.$

$\gcd(299, 345) = 23.$

$23 = 299 - 6(46)$

$23 = 299 - 6[345 - 299]$

$23 = 299 + 6(299) - 6(345)$

$23 = 7(299) - 6(345)$

2 (iii) For $d = \gcd(299, 345)$

and $23 = s(299) - t(345)$ — ①

let $x_0 = 7$ and $y_0 = -6$

in $ax + by = c.$

we want $s, t \in \mathbb{Z}^+$

$x = 7 + (\frac{345}{23})u$

$x = 7 + 15u$ and

$y = -6 - (\frac{299}{23})u$

$y = -6 - 13u$

For t in ① to be positive, we need the $y < 0.$

$-6 - 13u$ for $u \in \{0, 1, 2, \ldots\}$

(s,t): $(7, 6)$, $(22, 19)$, $(37, 32), \ldots$

NO: Divisibility Chapter 10.   DATE:

3. Assume on the first day, the train departs at 0:00 midnight. The we need to solve $7a = 9 + b(24)$.
i.e. $7a - b24 = 9$.
Since $\gcd(7,24) = 1$ and $1 | 9$ then there exist some integers s and t such that $7s + 24t = 9$.

$$24 = 3(7) + 3$$
$$7 = 2(3) + 1$$
$$3 = 3(1) + 0$$

Thus, $1 = 7 - 2(3)$.
$1 = 7 - 2[24 - 3(7)]$
$1 = 7 + 6(7) - 2(24)$
$1 = 7(7) - 2(24)$
So $9 = 9[7(7) - 2(24)]$
$9 = 63(7) - 18(24)$.
For $7x + 24y = 9$
$x = 63 + 24u$; $u \in \mathbb{Z}$
$y = -18 - 7u$
so $7(63 + 24u) - 24(18 + 7u) = 9$.
The coefficient of 24 increases by 7 units everytime.
Thus, Ivan can see Olga every 7 days.

If the train leaves every 14 hours then we need to solve $14a = 9 + 24b$; i.e. $14a - 24b = 9$.
Since $\gcd(14, 24) = 2$ but $2 \nmid 9$.
Thus, there are no integers s and t such that
$$14s + 24t = 9$$
i.e. No train ever leave at 9 am to Vladivostok.
But there is a train at some even time on some day say 12noon then $14a + 24b = 12$ and $2 | 12$
then there exist integers s and t such that $14s + 24t = 12$.
By inspection, $s_0 = 6$ and $t_0 = 3$. $s = 6 + \frac{24}{2}u$ and $t = 3 - \frac{14}{2}u$
so $t = -3 - 7u$; i.e. every 7 days, the train departs at noon.

NO:................................ DATE:................................

Useful Theorem If $\gcd(a,b)=d$ then
① $\gcd(\frac{a}{d}, \frac{b}{d})=1$
and ② $\gcd(a,b)=\gcd(a+cb, b)$;
$a,b,c \in \mathbb{Z}$.

Proof. ① Let $d=\gcd(a,b)$ and $e \in \mathbb{Z}$.
let $e \mid \frac{a}{d}$ and $e \mid \frac{b}{d}$ so
$\frac{a}{d}=ke$ and $\frac{b}{d}=le$, $k,l \in \mathbb{Z}$

$\Rightarrow a=kde$ and $b=lde$.
So a and b has a common divisor in de.
Since $d=\gcd(a,b)$ then $de \leq d$.
Thus, $e=1$.
So $\gcd(\frac{a}{d}, \frac{b}{d})=1$.
For ② we want to show that $\gcd(a,b) \Rightarrow \gcd(a+cb, b)$.
let e be a common divisor of a and b, $e \in \mathbb{Z}$.
$e \mid a$ and $e \mid b$
Thus, $e \mid (a+cb)$, $c \in \mathbb{Z}$.
$\Rightarrow$ e is a common divisor of b and $(a+cb)$ — ③
we want to show that $\gcd(a+cb, b) \Rightarrow \gcd(a,b)$.
let f be a common divisor of b and $(a+cb)$;
Then $f \mid (a+cb-cb) \Rightarrow f \mid a$
Thus, f is a common divisor of b and a. — ④

NO:.............................. DATE:..............................

4 Using the theorem that if $gcd(a,b) = d$ then

$gcd(a,b) = gcd(a+cb, b)$; $c \in \mathbb{Z}$

Show that $gcd(6n+8, 4n+5) = 1$; $n \in \mathbb{Z}^+$.

$\cancel{LHS} = gcd(6n+8, 4n+5)$

$= gcd((4n+5)+(2n+3), 4n+5)$

$= gcd(2n+3, 4n+5)$

$= gcd(2n+3, (2n+3)+(2n+2))$

$= gcd(2n+3, 2n+2)$

$= gcd((2n+2)+1, 2n+2)$

$= gcd(1, 2n+2)$

$= 1$

$= RHS$

5 Let $gcd(m,n) = 1$, $m|a$, $n|a$; $a, m, n \in \mathbb{Z}$.

Want to show that $(mn)|a$.

Since $m|a$ and $n|a$ then $a = km$ and $a = ln$

$k, l \in \mathbb{Z}$.

Thus, $km = ln$

Since $gcd(m,n) = 1$ then $n|k$

$k = pn$; $p \in \mathbb{Z}$

Thus, $a = km$

$= (pn)m$

$= p(mn)$

$\Rightarrow (mn)|a$ as required.

Let $gcd(3,6) = 2$ and $a = 24$.

$3|24$ and $6|24$

but $(3 \times 6) \nmid 24$.

NO: DATE: 10.6

6. let $d = \gcd(a,b)$ then there exist integers x and y such that $ax+by=d$ — ①

Next, we let $e = \gcd(d,c)$ then there exist integers p and q such that

$$dp + cq = e \quad \text{— ②}$$

By using ① and ② we have

$$(ax+by)p + cq = e$$

$$a(xp) + b(yp) + cq = e$$

Since $x, p, y, q \in \mathbb{Z}$ then $xp, yp, cq \in \mathbb{Z}$

let $s = xp$, $t = yp$ and $u = q$ then

$$sa + tb + cq = e$$

$$\Rightarrow \quad sa + tb + cq = \gcd(d, c)$$

$$= \gcd(\gcd(a,b), c)$$

$$= \gcd(a, b, c), \text{ as required.}$$

So $\gcd(91, 903, 1792) = \gcd(\gcd(91, 903), 1792)$

let $\gcd(91, 903) = d$

$903 = 9(91) + 84$

$91 = 1(84) + 7$

$84 = 12(7) + 0$

So $\gcd(91, 903, 1792) = \gcd(7, 1792)$

$1792 = 256(7) + 0$

So $\gcd(91, 903, 1792) = \underline{7}$

NO: Divisibility Chapter 10. DATE:

7 Let $3J + 4M = 7$ where 7 denotes a Sunday.
Since $\gcd(3,4) = 1$ and $1 \mid 7$ then there are integers x and y such that $3x + 4y = 7$.
By inspection,

$$7[3(-1) + 4(1)] = 7$$

So $x_0 = -1$ and $y_0 = 1$.

$$x = -1 + 4t \quad ; t \in \mathbb{Z}$$
$$y = 1 - 3t$$

So $7(3)(-1+4t) + 7(4)(1-3t) = 7$

$$21(-1+4t) + 28(1-3t) = 7$$

It will occur on a Sunday every $28(3) = \underline{84 \text{ days}}$.

8 Let $n \geq 2$, $n \in \mathbb{Z}$. Prove that
n is prime iff either $\gcd(a,n) = 1$ or $n \mid a$, for every $a \in \mathbb{Z}$

Proof

($\Rightarrow$) Let $n \geq 2$, $n \in \mathbb{Z}$, n is prime. Let $a \in \mathbb{Z}$

case ① a is a multiple of n.
i.e. $a = kn$; $k \in \mathbb{Z}$
thus, $n \mid a$.

case ② a is not a multiple of n.
i.e. $a = bn + q$; $b, q \in \mathbb{Z}$, $q \neq 0$
then $\gcd(a,n) = \gcd(bn+q, n)$
$= \gcd(q, n)$
Since q is a remainder in $a = bn + q$
then $0 < q < n$

Since $0 < q < n$ and n is prime then $\gcd(q,n) = 1$

($\Leftarrow$) Here we want to assume for every $a \in \mathbb{Z}$ and $\gcd(a,n) = 1$ or $n \mid a$ then n is prime.
Let for every integer a, $\gcd(a,n) = 1$ and n is an integer.
Case 1:
Proof by contradiction
Let for every integer a, $\gcd(a,n) = 1$, $n \nmid a$ and n is not a prime.

Since n is not a prime then $n = p_1 p_2 p_3 \cdots p_m$; $p_1, p_2, \ldots, p_m$ are some primes. • If $a < n$ then there exist an 'a' such that $a = p_1$ and $\gcd(a = p_1, p_1 p_2 \cdots p_m) = p_1 \neq 1$; where $p_1 < p_2 < \cdots < p_m$. which contradicts $\gcd(a, n) = 1$.

Thus, by the proof of contradiction, n is prime

• If $a \geq n$ then there exist an 'a' such that $a = kp_1$ where $k \in \mathbb{Z}^+$ and $\gcd(a = kp_1, p_1 p_2 \cdots p_m) = p_1 \neq 1$ which contradicts $\gcd(a, n) = 1$. Thus, by the proof of contradiction n is prime.

Case 2:

proof by contradiction.

Let for every integer a, $n | a$ and n is not a prime.

Since n is not a prime then $n = p_1 p_2 \cdots p_m$; $p_1, p_2, \ldots, p_m$ are some primes.

Since for every integer a, $n | a$ then $a = k p_1 p_2 \cdots p_m$; and $a + 1 = (k p_1 p_2 \cdots p_m) + 1$ where $k \in \mathbb{Z}$

but $n \nmid [(k p_1 p_2 \cdots p_m) + 1]$ which contradicts $n | a$ for every integer a.

Thus, by the proof of contradiction, n is prime.

Thus, the statement is shown as required

9 Let $\gcd(a, b) = 1$ then there exist integers x and y such that $xa + yb = 1$ —— ①. Multiply both sides of ① with any integer n to obtain $nxa + nyb = n$

Let $s = nx$ and $t = ny$ so that $sa + tb = n$.

$\Rightarrow sa = (n - tb)$

$\Rightarrow s = \frac{(n - tb)}{a}$ since $a > 0$ then when $n - tb > 0$

$\Rightarrow n > tb$

$\Rightarrow \frac{n}{b} > t$

we have $s > 0$.

So there exist integers s, t with $s > 0$ such that $sa + tb = n$ for any integer n.

10. We want to prove that for any integer $n > 23$, there exist non-negative integers x and y such that $4x + 9y = n$.

Let us consider $n = 24$.

$4x + 9y = 24$

By inspection, $x_0 = 6$, $y_0 = 0$.

$$\left.\begin{aligned} x &= 6 + 9t \\ y &= -4t \; ; \; t \in \mathbb{Z} \end{aligned}\right\} \quad ①$$

We know consider $n = 24 + k$; where k is some known constant and $k \in \{0, 1, 2, \ldots\}$

So $4x' + 9y' = 24 + k$ and since $\gcd(4,9) = 1$

then there exists integer a, b such that $4a + 9b = 1$.

by inspection $4(-2) + 9(1) = 1$

so $k[4(-2) + 9(1)] = k$

$4(-2k) + 9(k) = k$ — ②

So $4x' + 9y' = 24 + k$ can be written as

$(4x + 9y) + k = 24 + k$ and by ① and ②, we have

$4(6+9t) + 9(-4t) + 4(-2k) + 9(k) = 24 + k$

$4(6 + 9t - 2k) + 9(k - 4t) = 24 + k$.

We want $6 + 9t - 2k \geq 0$ and $k - 4t \geq 0$.

$9t \geq 2k - 6$ $\qquad$ $k \geq 4t$

$t \geq \frac{(2k-6)}{9}$ $\qquad$ $\frac{k}{4} \geq t$

Check if $k = 2$ then $t \geq \frac{2(2)-6}{9}$ and $\frac{1}{2} \geq t$

$t \geq \frac{-2}{9}$

so $t = 0$.

Then $x = 6 + 9(0) - 2(2)$ and $y = 2 - 4(0)$

$x = 2$ $\qquad$ $y = 2$

$4(2) + 9(2) = 8 + 18$

$= 26$ checked out to be right.

We now want to show that there is no non-negative integers x and y such that $4x + 9y = 23$

We will consider all cases of non-negative integers x and y.

x	y	$4x+9y$	equal to 23
0	0	$4(0)+9(0)=0$	No
0	1	$4(0)+9(1)=9$	No.
0	2	$4(0)+9(2)=18$	No.
0	3	$4(0)+9(3)=27 > 23$	No
1	0	$4(1)+9(0)=4$	No.
2	0	$4(2)+9(0)=8$	No.
3	0	$4(3)+9(0)=12$	No.
4	0	$4(4)+9(0)=16$	No.
5	0	$4(5)+9(0)=20$	No.
6	0	$4(6)+9(0)=24 > 23$	No.
1	1	$4(1)+9(1)=13$	No.
2	1	$4(2)+9(1)=17$	No.
3	1	$4(3)+9(1)=21$	No.
4	1	$4(4)+9(1) > 23$	No.
1	2	$4(1)+9(2)=22$	No.
2	2	$4(2)+9(2)=26 > 23$	No.

Note $x=0$, $y \geq 3$ then $4x+9y > 23$.
$x \geq 6$, $y=0$ then $4x+9y > 23$
$x \geq 2$, $y=2$ then $4x+9y > 23$
and $x \geq 4$, $y=1$ then $4x+9y > 23$.

Thus, there is no non-negative integers x and y such that $4x+9y = 23$.

cont. of 10.10

Notice that for $4x+9y=23$
$23 = 4(9)-(4+9)$.

Thus, we conjecture that for any pair a,b of relatively positive primes; $N = ab-(a+b)$; $a,b \in \mathbb{Z}^+$, and

$$n \geq N+1$$
$$n \geq ab-(a+b)+1$$
$$n \geq ab-a-b+1$$
$$n \geq a(b-1)-(b-1)$$
$$n \geq (a-1)(b-1)$$

That is, for any integer $n \geq (a-1)(b-1)$ it is possible to find integers $s,t \geq 0$ satisfying $sa+tb=n$, but no such s,t exist satisfying $sa+tb=ab-(a+b)$.

I leave the proof to you.

11 (ai) Let $a,b,c,d \in \mathbb{Z}$.
Let $a|b$ then $b=ka$; $k\in\mathbb{Z}$
Consider bc.
Since $b=ka$ then $bc=(ka)c$
$=(kc)a$
Since, $k,c\in\mathbb{Z}$ then $(kc)\in\mathbb{Z}$
Thus, $a|(bc)$ as required.

(aii) Let $a|b$ and $a|c$.
i.e. $b=ka$ and $c=la$; $k,l\in\mathbb{Z}$
Consider bc.
Since $b=ka$ and $c=la$ then $bc=kala$
$=(kl)a^2$
Since, $k,l\in\mathbb{Z}$ then $(kl)\in\mathbb{Z}$.
Thus, $a^2|(bc)$ as required

(aiii) Let $a|b$ and $c|d$, $c\neq 0$ then
$b=ka$ and $d=lc$; $k,l\in\mathbb{Z}$
Consider bd.
Since $b=ka$ and $d=lc$ then $bd=(kl)ac$
Since, $k,l\in\mathbb{Z}$ then $(kl)\in\mathbb{Z}$
Thus, $(ac)|(bd)$ as required

(aiv) Let $a|b$ then $b=ka$; $k\in\mathbb{Z}$
Consider $b^n=(ka)^n$
$=k^na^n$
Since $k\in\mathbb{Z}$ then $k^n\in\mathbb{Z}$.
Thus, $a^n|b^n$ as required

11b. Note
If $p\Rightarrow q$ then its converse is
$q\Rightarrow p$.
So the converse of a(iv) is
If $a^n|b^n$ then $a|b$.
Let $a^n|b^n \Rightarrow b^n=ka^n$, $k\in\mathbb{Z}$.
and n is a natural number.
So $k=(b/a)^n$
Since k is a positive integer and n is a natural number then (b/a) must be an integer h.
So $b=ah$
Thus, $a|b$.

12. Let $k\in\mathbb{Z}$
Consider k, $k+2$, $k+4$
Case 1: If $3|k$ then one of $k,k+2,k+4$ is divisible by 3
Case 2: If $3\nmid k$ then
$k+1$ or $k+2$ is divisible by 3
If $k+2$ is divisible by 3 then one of $k,k+2,k+4$ is divisible by 3.
If $k+1$ is divisible by 3 then let $k+1=3p$; $p\in\mathbb{Z}$
then $k+4=k+1+3$
$=3p+3$ which is divisible by 3 then one of $k,k+2,k+4$ is divisible by 3.

NO: DATE: 10.12

13. Let P : If $p \mid (q+r)$ then either $p \mid q$ or $p \mid r$

Let $p, q, r \in \mathbb{Z}$.

Counter example

Let $p = 8$, $q = 13$ and $r = 3$

Then $8 \mid (13+3)$ but $8 \nmid 13$ and $8 \nmid 3$

So the statement P is not true.

14. Let $\gcd(a,b) = 1$ and $c \mid a$; $a, b, c \in \mathbb{Z}$

Since $\gcd(a,b) = 1$ then there exist integers s and t such that $1 = sa + tb$.

Since $c \mid a$ then $a = kc$, $k \in \mathbb{Z}$.

Thus, $1 = sa + tb$ can be re-written as

$$1 = s(kc) + tb$$

$$1 = (sk)c + tb$$

Since $s, k \in \mathbb{Z}$ then $(sk) \in \mathbb{Z}$.

Thus, $\gcd(c,b) = 1$ as required.

15. Let $\gcd(a,b) = 1$; $a, b \in \mathbb{Z}$

Since $\gcd(a,b) = 1$ then there exist integers s and t such that $1 = sa + tb$ — ①

From ① $1 = (sa + tb)^2$

$$= s^2a^2 + t^2b^2 + 2st\,ab \quad — ②$$

$$= s^2a^2 + (t^2b + 2sta)b$$

Since $s, t \in \mathbb{Z}$ then $s^2 \in \mathbb{Z}$, $t^2b + 2sta \in \mathbb{Z}$.

Thus, $\gcd(a^2, b) = 1$ as required.

Note for question 15

Definition

$$d = \gcd(a,b) \iff d \in \mathbb{Z}^+ \quad (1)\ d|a \text{ and } d|b \quad (2) \text{ if } e|a \text{ and } e|b \text{ then } e|d.$$

① says that the greatest common divisor divides both a and b by definition and
② says that if there exists a divisor e that divides a and b then it must be the case that e also divides d; i.e. e as a common divisor is smaller in magnitude to d; the greatest common divisor.

---

15. ② can also be written as

$$1 = (s^2a + 2stb)a + t^2b^2$$

Since $s, t, a, b \in \mathbb{Z}$ then $(s^2a + 2stb) \in \mathbb{Z}$ and $t^2 \in \mathbb{Z}$.
Thus, $\gcd(a, b^2) = 1$ as required.

Thus, $a^2p_1 + bp_1 = 1 \ \ldots$ ③
$aq_1 + b^2q_2 = 1 \ \ldots$ ④ ; $p_1, p_2, q_1, q_2 \in \mathbb{Z}$

from ① $ab(sa + tb) = ab$ — ⑤
from ③ $a(a^2p_1 + bp_1) = 1(a)$
$a^3p_1 + abp_1 = a$ — ⑥
Substitute ⑤ into ⑥

$$a^3p_1 + ab(sa + tb)p_1 = a$$
$$a^3p_1 + a^2bs + atp_1b^2 = a$$

and in ④

$$(a^3p_1 + a^2bs + atp_1b^2)q_1 + b^2q_2 = 1$$
$$a^2(ap_1 + bs) + b^2(atp_1q_1 + q_2) = 1$$

since $(ap_1 + bs) \in \mathbb{Z}$ and $(atp_1q_1 + q_2) \in \mathbb{Z}$ then
$\gcd(a^2, b^2) = 1$.

10.14

NO:............................ DATE:............................

16 Let $\gcd(a,b)=1$; $a,b \in \mathbb{Z}$ and let $a > b$.
Since $\gcd(a,b)=1$ then $1|a$ and $1|b$.

Case 1: Consider $S_1 = a+b + (a-b)$
$S_1 = 2a$
Thus, $\gcd(a+b, a-b) = 2$

Case 2: Consider $S_2 = a+b-(a-b)$.
$S_2 = 2b$
Thus, $\gcd(a+b, a-b) = 2$

Case 3: Consider $u = m(a+b) + n(a-b)$
$u = a(m+n) + b(m-n)$
Since $1|a$ and $1|b$ then $1|[a(m+n)+b(m-n)]$
Thus, $\gcd(a+b, a-b) = 1$

Thus, $\gcd(a+b, a-b) = 1$ or 2.