Number Theory

Problem 1

How many numbers are there between 100 and 1000 that are

(a) divisible by 3?

(b) divisible by 5?

(c) divisible by 15?

Solution

Using the formula $\left\lfloor \frac{m}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor$:

(a) $\left\lfloor \frac{1000}{3} \right\rfloor - \left\lfloor \frac{99}{3} \right\rfloor = 300$ numbers divisible by 3 $(102, 105, \ldots, 999)$;

(b) $\left\lfloor \frac{1000}{5} \right\rfloor - \left\lfloor \frac{99}{5} \right\rfloor = 181$ numbers divisible by 5 $(100, 105, \ldots, 1000)$;

(c) $\left\lfloor \frac{1000}{15} \right\rfloor - \left\lfloor \frac{99}{15} \right\rfloor = 60$ numbers divisible by 15 $(105, 120, \ldots, 990)$.

Problem 2

(a) What is:

- (i) $\gcd(420, 720)$?
- (ii) $\operatorname{lcm}(420, 720)$?
- (iii) $720 \text{ div } 42$?
- (iv) $5^{20} \;\%\; 7$?

(b) True or false:

- (i) $42 | 7$?
- (ii) $7 | 42$?
- (iii) $3 + 5 | 9 + 23$?
- (iv) $27 =_{(6)} 33$?
- (v) $-1 =_{(7)} 22$?

Solution

(a) (i) Using the Faster Euclidean Algorithm:

$$\begin{aligned}
\gcd(420, 720) &= \gcd(420, 720 \% 420) &&= \gcd(420, 300) \\
&= \gcd(420 \% 300, 300) &&= \gcd(120, 300) \\
&= \gcd(120, 300 \% 120) &&= \gcd(120, 60) \\
&= \gcd(120 \% 60, 60) &&= \gcd(0, 60) \\
&= 60
\end{aligned}$$

(ii) We have:

$$\mathrm{lcm}(420, 720) = \frac{420 \cdot 720}{\gcd(420, 720)} = \frac{302400}{60} = 5040.$$

(iii) We have:

$$720 \text{ div } 42 = \left\lfloor \frac{720}{42} \right\rfloor = 17.$$

(iv) We have:

$$5^3 = 125 =_{(7)} 6 =_{(7)} -1.$$

So,

$$5^6 = (5^3)^2 =_{(7)} (-1)^2 = 1.$$

Therefore,

$$5^{20} = 5^2 \cdot 5^{18}) = 5^2 \cdot (5^6)^3 =_{(7)} 25 \cdot 1^3 =_{(7)} 4,$$

so $5^{20} \% 7 = 4 \% 7 = 4$.

(b) (i) False because there is no integer k such that $7 = 42k$.

(ii) True because $42 = 6 \cdot 7$

(iii) True because $9 + 23 = 32 = 4 \cdot 8 = 4(3 + 5)$

(iv) True because $6 | (33 - 27)$: $33 - 27 = 6 = 1 \cdot 6$.

(v) False because $7 \nmid (-1 - 22)$: $(-1 - 22) = -23 = -4 \cdot 7 + 5$

Problem 3† (2020 T2)

Prove, or give a counterexample to disprove:

(a) For all $x \in \mathbb{R}$:

$$|\lfloor x \rfloor| = \lfloor |x| \rfloor$$

(b) For all $x \in \mathbb{Z}$:

$$42 | x^7 - x$$

(c) For all $x, y, z \in \mathbb{Z}$, with $z > 1$ and $z \nmid y$:

$$(x \text{ div } y) =_{(z)} ((x \% z) \text{ div } (y \% z))$$

Solution

(a) This is false, consider $x = -0.5$:

$$|\lfloor x \rfloor| = |\lfloor -0.5 \rfloor| = |-1| = 1,$$

but

$$\lfloor |x| \rfloor = \lfloor |-0.5| \rfloor = \lfloor 0.5 \rfloor = 0.$$

(b) We will first show that for all x, $2|x^7 - x$, $3|x^7 - x$, and $7|x^7 - x$.

NB

Since

$$x^7 - x = (x^2 - x)(x^5 + x^4 + x^3 + x^2 + x + 1) = (x^3 - x)(x^4 + x^2 + 1),$$

this result can be established with Fermat's little theorem.

For all $x \in \mathbb{Z}$, we have either $x \% 2 = 0$ or $x \% 2 = 1$.

- If $x \% 2 = 0$, then $x^7 =_{(2)} 0^7 =_{(2)} 0 = x$
- If $x \% 2 = 1$, then $x^7 =_{(2)} 1^7 =_{(2)} 1 = x$

Therefore, for all $x \in \mathbb{Z}$, we have $x^7 =_{(2)} x$, so $2|x^7 - x$.
For all $x \in \mathbb{Z}$, we have either $x \% 3 = 0$, $x \% 3 = 1$, or $x \% 3 = 2$.

- If $x \% 3 = 0$, then $x^7 =_{(3)} 0^7 =_{(3)} 0 = x$
- If $x \% 3 = 1$, then $x^7 =_{(3)} 1^7 =_{(3)} 1 = x$
- If $x \% 3 = 2$, then $x^7 =_{(3)} 2^7 =_{(3)} 126 + 2 =_{(3)} 2 = x$

Therefore, for all $x \in \mathbb{Z}$, we have $x^7 =_{(3)} x$, so $3|x^7 - x$.
Finally, for all $x \in \mathbb{Z}$, we have either $x =_{(7)} 0$, $x =_{(7)} \pm 1$, $x =_{(7)} \pm 2$, or $x =_{(7)} \pm 3$.

- If $x \% 7 = 0$, then $x^7 =_{(7)} 0^7 =_{(7)} 0 = x$
- If $x \% 7 = \pm 1 \% 7$, then $x^7 =_{(7)} (\pm 1)^7 =_{(7)} \pm 1 = x$
- If $x \% 7 = \pm 2 \% 7$, then $x^7 =_{(7)} (\pm 2)^7 =_{(7)} \pm 128 =_{(7)} \pm 2 = x$
- If $x \% 7 = \pm 3 \% 7$, then $x^7 =_{(7)} (\pm 3)^7 =_{(7)} \pm 2187 =_{(7)} \pm 3 = x$

Therefore, for all $x \in \mathbb{Z}$, we have $x^7 =_{(7)} x$, so $7|x^7 - x$.
We will now show that if $2|k$, $3|k$, and $7|k$ then $42|k$.
Suppose $2|k$, $3|k$, and $7|k$.

- Since $2|k$, $k = 2m$ for some $m \in \mathbb{Z}$.
- Since $3|k$, we have $3|2m$, so $0 =_{(3)} 2m$. Therefore,

  $$0 = 2 \cdot 0 =_{(3)} 2 \cdot 2m =_{(3)} 4m =_{(3)} m.$$

  So $m = 3p$ for some integer p, and hence $k = 2m = 6p$.

- Since $7|k$, we have $7|6p$, so $0 =_{(7)} 6p$. Therefore,

$$0 = 6 \cdot 0 =_{(7)} 6 \cdot 6p =_{(7)} 36p =_{(7)} p.$$

So $p = 7q$ for some integer q, and hence $k = 42q$, so $42|k$.

(c) This is false. Consider $x = 4$, $y = 3$, $z = 2$: then

- $x \text{ div } y = 4 \text{ div } 3 = 1$,
- $x \% z = 4 \% 2 = 0$,
- $y \% z = 3 \% 2 = 1$,
- $(x \% z) \text{ div } (y \% z) = 0 \text{ div } 1 = 0$, and so
- $x \text{ div } y \neq_{(z)} (x \% z) \text{ div } (y \% z)$

Problem 4
Prove that for all $m, n, p \in \mathbb{Z}$ with $n \geq 1$:

(a) $0 \leq (m \% n) < n$

(b) $m =_{(n)} p$ if, and only if $(m \% n) = (p \% n)$

Solution

(a) We first observe that for all $x \in \mathbb{R}$, $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. This follows from the definition of $\lfloor \cdot \rfloor$ as being the greatest integer that is less than or equal to x. As $\lfloor x \rfloor + 1$ is also an integer that is greater than $\lfloor x \rfloor$, it must be greater than x.

We then have for all $m, n \in \mathbb{Z}$:

$$\begin{array}{rll} \lfloor \frac{m}{n} \rfloor & \leq \frac{m}{n} & < \lfloor \frac{m}{n} \rfloor + 1 \\ \text{So, } n \cdot \lfloor \frac{m}{n} \rfloor & \leq n \cdot \frac{m}{n} & < n \cdot (\lfloor \frac{m}{n} \rfloor + 1) \\ \text{So, } n \cdot \lfloor \frac{m}{n} \rfloor & \leq m < n + n \cdot \lfloor \frac{m}{n} \rfloor & \\ \text{So, } 0 & \leq m - (n \cdot \lfloor \frac{m}{n} \rfloor) & < n \text{ as required.} \end{array}$$

(b) We first observe that $x =_{(n)} (x \% n)$ because $x - (x \% n) = x - (x - n \cdot \lfloor \frac{x}{n} \rfloor) = n \cdot \lfloor \frac{x}{n} \rfloor$, so $n | x - (x \% n)$.

If $m =_{(n)} p$, then

$$(m \% n) \quad =_{(n)} \quad m \quad =_{(n)} \quad p \quad =_{(n)} \quad (p \% n)$$

Therefore $n|((m \% n) - (p \% n))$.

From (a) we have $(m \% n), (p \% n) \in [0, n)$, so $((m \% n) - (p \% n)) \in (-n, n)$.

The only multiple of n in the interval $(-n, n)$ is 0, so $(m \% n) = (p \% n)$.

Conversely, if $(m \% n) = (p \% n)$, then

$$m \quad =_{(n)} \quad (m \% n) \quad =_{(n)} \quad (p \% n) \quad =_{(n)} \quad p.$$

NB

We are implicitly using the observation that $=_{(n)}$ is transitive.

Problem 5

Suppose $m =_{(n)} m'$ and $p =_{(n)} p'$. Prove that:

(a) $m + p =_{(n)} m' + p'$

(b) $m \cdot p =_{(n)} m' \cdot p'$

Solution

We have $n | m - m'$ and $n | p - p'$, so let $m - m' = kn$ and $p - p' = jn$. Then:

(a) $(m + p) - (m' - p') = (m - m') + (p - p') = kn + jn = (k + j)n$, so $n | (m + p) - (m' - p')$. That is,

$$m + p =_{(n)} m' + p'$$

(b) $mp - m'p' = mp - m'p + m'p - m'p' = (m - m')p + m'(p - p') = knp + m'jn = (kp + jm')n$, so $n | mp - m'p'$. That is,

$$m \cdot p =_{(n)} m' \cdot p'$$

Problem 6

(a) Prove that the 4 digit number $n = abcd$ is:

(i) divisible by 5 if and only if the last digit d is divisible by 5.

(ii) divisible by 9 if and only if the digit sum $a + b + c + d$ is divisible by 9.

(iii) divisible by 11 if and only if $a - b + c - d$ is divisible by 11.

(b) Find a similar rule to determine if a 4 digit number is divisible by 7.

Solution

We observe that $n = a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d$. Therefore:

(a) (i) $n =_{(5)} a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d =_{(5)} a \cdot 0^3 + b \cdot 0^2 + c \cdot 0 + d =_{(5)} d$. So n is divisible by 5 (i.e. $n =_{(5)} 0$) if, and only if d is divisible by 5.

(ii) $n =_{(9)} a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d =_{(9)} a \cdot 1^3 + b \cdot 1^2 + c \cdot 1 + d =_{(9)} a + b + c + d$. So n is divisible by 9 (i.e. $n =_{(9)} 0$) if, and only if $a + b + c + d$ is divisible by 9.

(iii) $n =_{(11)} a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d =_{(11)} a \cdot (-1)^3 + b \cdot (-1)^2 + c \cdot (-1) + d =_{(11)} -a + b - c + d = -(a - b + c + d)$. So n is divisible by 11 (i.e. $n =_{(11)} 0$) if, and only if $a - b + c - d$ is divisible by 11.

(b) Observing that $10 =_{(7)} 3$, $10^2 =_{(7)} 3^2 =_{(7)} 9 =_{(7)} 2$, and $10^3 =_{(7)} 3 \cdot 2 =_{(7)} 6 =_{(7)} -1$ we can state one divisibility by 7 rule (there are others) as:

n is divisible by 7 if, and only if $-a+2b+3c+d$ is divisible by 7.

Problem 7† (2020 T3)

The following process leads to a rule for determining if a large number n is divisible by 17:

- Remove the last digit, b, of n leaving a smaller number a.
- Let $n' = a - 5b$.
- Repeat with n' in place of n.

So, for example, if $n = 12345$, then $n' = 1234 - 5 \cdot 5 = 1209$. Repeating would create $120 - 5 \cdot 9 = 75$; $7 - 5 \cdot 5 = -18$; and so on.

Prove that $17|n$ if and only if $17|n'$.

Problem 8*

Prove that for $m, n \in \mathbb{Z}$:

$$\gcd(m,n) \cdot \operatorname{lcm}(m,n) = |m| \cdot |n|$$

Problem 9*

Prove that for all $n \in \mathbb{Z}$:

$$\gcd(n, n+1) = 1.$$

Solution

Suppose $x|n$ and $x|n+1$. Then $x|(n+1)-n$, so $x|1$. Therefore the only common factors of n and $n+1$ are ± 1, and hence $\gcd(n, n+1) = 1$. Note that this applies for any $n \in \mathbb{Z}$

Problem 10*

Prove that for all $x, y, z \in \mathbb{Z}$:

$$\gcd(\gcd(x,y),z) = \gcd(x, \gcd(y,z)).$$

Solution

We will first show that $\gcd(\gcd(x,y),z) = \gcd(x,y,z)$.

Let $d = \gcd(x,y,z)$, $e = \gcd(x,y)$ and $f = \gcd(e,z)$.
We have $d|x$, $d|y$ and $d|z$, and d is the greatest integer which is a common divisor of all three.
Since $d|x$ and $d|y$, we have, from Bézout's identity (see Assignment) that $d|e$.
As $d|e$ and $d|z$, we have that d is a common factor of e and z, so $d \leq f$.

We also have that $f|e$ and $e|x$ so $f|x$; and $e|y$, so $f|y$.

Hence $f|x$, $f|y$, and $f|z$, so $f \leq d$.

Therefore $f = d$, so $\gcd(\gcd(x,y),z) = \gcd(x,y,z)$

Following the claim we have:

$$\gcd(\gcd(x,y),z) = \gcd(x,y,z) = \gcd(y,z,x) = \gcd(\gcd(y,z),x) = \gcd(x,\gcd(y,z)),$$

as required.