Examples related to the homework / How to use the fundamental Theorem of arithmetic :

#1

$a \equiv r \pmod n$, $b \equiv s \pmod n$, $a - r = nq_1$, $b - s = nq_2$, $q_1, q_2 \in \mathbb{Z}$

$\Updownarrow$

$a + b - (r+s) = nk_1$ $\quad$ $ab - rs = nk_2$

$\therefore$ $a+b \equiv r+s \pmod n$ $\quad$ $\therefore$ $ab \equiv rs \pmod n$

$[a+b] = [r+s]$ $\quad$ $[a][b] = [ab] = [rs] = [r][s]$

#2

a) Last digit of 7^{2023} :

In $\mathbb{Z}_{10}$

$[7^{2023}] = [7]^{2023}$

$= [-3]^{2023} = ([-3]^2)^{1011}([-3])$

$= ((-3)^2)^{1011}[-3]$

$= [9]^{1011}[-3]$

$= [-1]^{1011}[-3]$ $\rightarrow$ $0, \cdots, 9$

$= [-1][-3] = [3]$

$2 \overline{)2023}$ 1011, 2022, 1

Last digit $123 = 10 \times 12 + 3$

the remainder of 123 divided by 10

Last digit: $12456 = 10 \times 1245 + 6 \equiv$ is the remainder when this no is divided by 10

$\mathbb{Z}_{28}$ $[\ ] = - = [\ ]$

#3 In $\mathbb{Z}_3$ If $[abc-1] = [0]$, then i.e., $[abc] = [1]$ ...

$[a-1]$, $[b-1]$ or $(c-1)$ is $[0]$

$0, 1, \cdots, 27$.

$3n+2$, $n+1$ are coprime

$\gcd(3n+2, n+1) = 1$.

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

$= 1$.

$a, b \in \mathbb{Z}$ are relatively prime/coprime if $\gcd(a,b) = 1$.

Application of F.T. of Arithmetic:

$\log_{10} 57$ is not natural.

Assume not. $\log_{10} 57 = \frac{m}{n}$, $m, n \in \mathbb{N}$

$\therefore \quad 57 = 10^{\frac{m}{n}}$.

$(3 \times 19)^m = 57^n = 10^m = 2^m 5^m$

$\log_{10} 7 = \frac{-m}{n}$, $m, n \in \mathbb{N}$.

$7 = 10^{\frac{-m}{n}}$

$7^n = 10^{-m}$

$10^m 7^n = 1$

$5^{\frac{1}{7}} = \frac{m}{n}$ $\quad m, n \in \mathbb{N}$

$5 = \left(\frac{m}{n}\right)^7$

$5 \cdot (p_1 \cdots p_r)^7 = 5n^7 = m^7 = (q_1 \cdots q_s)^7$

11.5 Relatively Prime Integers

Definition Let $a, b \in \mathbf{Z}$, not both zero. Then they are relatively prime if $\gcd(a, b) = 1$.

Theorem Let $a, b \in \mathbf{Z}$, not both zero. Then $\gcd(a, b) = 1$ if and only if there are $x, y \in \mathbf{Z}$ such that $ax + by = 1$.

Question. How to find x and y?

(3) If ~~there~~ ax

~~Let a,~~

($\Leftarrow$) Let $a, b \in \mathbb{Z}$ non-zero

If there are $x, y \in \mathbb{Z}$ s.t.

$ax + by = 1$

Then $1 = \gcd(a, b)$

i.e., a, b are copmie

are relatively prime.

($\Rightarrow$) Clear.

Remark:

(1) Given $a, b \in \mathbb{Z}$.

If there are $x, y \in \mathbb{Z}$.

$ax + by = 10$.

Then we know.

that

$d = \gcd(a, b)$

~~Satis~~ is a factor

of 10.

(2) If $d = \gcd(a, b)$,

then

$d = ax + by$.

and for any

$md = a(mx) + b(my)$

$a, b \in \mathbb{Z}$.

Proof: $d = \gcd(a,b)$. ← $d \mid a \wedge d \mid b$; any common divisor $\hat{d}$ of a & b satisfies $\hat{d} \le d$

Then

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

(b) $d = \min\{ax+by : x, y \in \mathbb{Z}, ax+by > 0\}$.

Fact: every number of the form $ax+by$ is a multiple of d.

~~(c)~~

Suppose $d = \gcd(a,b)$.

We show that

$d = \min\{ax+by : x, y \in \mathbb{Z}, ax+by > 0\}$

(3) $d \mid (ax+by)$ for any $x, y \in \mathbb{Z}$.

~~Suppose~~ Only only need to show

$\hat{d} = \min\{ax+by : x, y \in \mathbb{Z}, ax+by > 0\}$

satisfies. (a) (1) $\hat{d} \mid a$, $\hat{d} \mid b$

(b) (2) $\hat{d}$ is larger than any common divisor.

~~(3)~~

Assume $\hat{d} \nmid a$.

Then $a = \hat{d}q + r$, $r = 1, 2, \cdots, \hat{d}-1$.

via (3)

Then $\hat{d} = ax+by$ for some $x, y \in \mathbb{Z}$.

So $r = a - \hat{d}q = a - (ax+by)q = a(1-xq) + b(-qy) \in S$

$r < \hat{d}$, which is contradiction ∵ $\hat{d} \nmid a$ is not true

∴ $\hat{d} \mid a$

Next, we show $\hat{d} \mid b$. Assume not

Then $b = \hat{d} q_2 + r_2$, $r_2 = 1, 2, \cdots, \hat{d}-1$.

So $r_2 = b - \hat{d} q_2$

$= b - (ax+by) q_2$

$= a(-xq_2) + b(1 - yq_2) \in S$.

& $r_2 < \hat{d}$, which is impossible.

So $\hat{d} \mid b$

---

(3) If there is $c = a\hat{x} + b\hat{y} \in S$ such that c is not a multiple of $\hat{d}$,

then $\hat{c} = \hat{d} q_3 + r_3$. $r_3 = 1, \cdots, \hat{d}-1$.

So $r_3 = \hat{c} - \hat{d} q_3 = (a\hat{x} + b\hat{y}) - (ax+by) q_3$

$= a(\hat{x} - xq_3) + b(\hat{y} - yq_3)$

$\in S$.

$r_3 < \hat{d}$, which is impossible.

(2) If l is a common divisor of a & b.

then $a = lk_1$, $b = lk_2$.

$\hat{d} = ax + by = lk_1x + lk_2y = l(k_1x + k_2y)$.

$\hat{d} = lz$

$|\hat{d}| = |l||z|$

$\geq |l|$

$\therefore l \leq \hat{d}$

Theorem (Euclid's Lemma) If $a|(bc)$ and $\gcd(a,b)=1$, then $a|c$.

Corollary Let p is a prime. If $p|bc$, then $p|b$ or $p|c$. More generally, for any integers $a_1,\dots,a_n$ with $n\geq 2$, if $p|a_1\cdots a_n$ then $p|a_i$ for some $i\in\{1,\dots,n\}$.

Theorem Let $a,b,c\in\mathbf{Z}$ such that $ab\neq 0$ and $\gcd(a,b)=1$. If $a|c$ and $b|c$, then $(ab)|c$.

Proof of Theorem. Assume $a|(bc)$, $\gcd(a,b)=1$.

$bc=al$, $l\in\mathbb{Z}$

$\gcd(a,b)=1$, i.e. $ax+by=1$ for some $x,y\in\mathbb{Z}$

$c=c\cdot 1=c(ax+by)=acx+bcy=acx+aly=a(cx+ly)$

$\therefore\ c=ak$ $k\in\mathbb{Z}$ with $k=cx+ly$.

$\therefore\ a|c$.

Let $a,b\in\mathbb{Z}$.

Proof $ab\neq 0$, $\gcd(a,b)=1$, $a|c$, $b|c$.

There are $x,y\in\mathbb{Z}$ $ax+by=1$, $c=aq_1=bq_2$.

$c=cq=aq_1(ax+by)=aq_1ax+abq_1y$

$c(ax+by)$

$c=abk$.

$\therefore\ (ab)|c$

$c=aq_1=bq_2$

$\therefore\ b|aq_1$ $\therefore\ b|q_1$ $\because$ gcd $\gcd(a,b)=1$

11.6 The Fundamental Theorem of Arithmetic

Theorem Every integer $n \geq 2$ is a product of primes $p_1 \cdots p_m$. The factorization is uniques up to a rearrangement of $p_1, \ldots, p_m$. That is: if n is a product of primes $q_1 \cdots q_r$, then $r = m$, and $q_1, \ldots, q_m$ is a rearrangement of $p_1, \ldots, p_m$.

Suppose $p_1 \cdots p_m = q_1 \cdots q_r$.

Step 1. Show $p_1 = q_i$ for some i by Euclid Lemma.

$\therefore$ $p_2 \cdots p_m = q_1 \cdots q_{i-1} \hat{q_i} q_{i+1} \cdots q_r$.

By induction on m, we see that every p_i appears in the list $q_1, \ldots, q_r$.

Now Reverse the roles of $q_1, \ldots, q_r$ & $p_1 \cdots p_m$

We can show q_1 is one of the p_j's.

$\therefore$ $q_2 \cdots q_r = p_1 \cdots p_{j-1} \hat{p_j} p_{j+1} \cdots p_m$.

By induction on r, we see that every q_j appears in the list $p_1, \ldots, p_m$.