

① gcd of 312 and 45

HW 1

Solution

$$312 = 6 \cdot 45 + 42$$

$$45 = 1 \cdot 42 + 3$$

$$42 = 14 \cdot 3 + 0$$

$$(312, 45) = 3$$

Answer

② Find  $(x, y)$  s.t.

$$221x + 77y = 1$$

First, gcd of 221 and 77:

$$221 = 2 \cdot 77 + 67$$

$$77 = 1 \cdot 67 + 10$$

$$67 = 6 \cdot 10 + 7$$

$$10 = 1 \cdot 7 + 3$$

$$7 = 2 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

$(221, 77) = 1 \Rightarrow$  such  $x$  and  $y$   
actually exist!

Backtrack:  $1 = 7 - 2 \cdot 3$

$$= 7 - 2(10 - 1 \cdot 7)$$

$$= 3 \cdot 7 - 2 \cdot 10$$

$$= 3(67 - 6 \cdot 10) - 2 \cdot 10$$

$$= 3 \cdot 67 - 20 \cdot 10$$

$$= 3 \cdot 67 - 20(77 - 1 \cdot 67)$$

$$= 23 \cdot 67 - 20 \cdot 77$$

$$= 23(221 - 2 \cdot 77) - 20 \cdot 77$$

$$1 = 23 \cdot 221 - 66 \cdot 77$$

Answer:

$$\begin{cases} x = 23 \\ y = -66 \end{cases}$$

③ Find  $x, y$  s.t.  $46x + 32y = -4$

Find gcd  $(46, 32)$

$$46 = 1 \cdot 32 + 14$$

$$32 = 2 \cdot 14 + 4$$

$$14 = 3 \cdot 4 + \boxed{2}$$

$$4 = 2 \cdot 2 + 0$$

$$\therefore (46, 32) = 2$$

Since  $-4$  is a multiple of 2,  
such  $x$  and  $y$  exist.

$$\begin{aligned} 2 &= 14 - 3 \cdot 4 \\ &= 14 - 3(32 - 2 \cdot 14) \\ &= 7 \cdot 14 - 3 \cdot 32 \\ &= 7(46 - 1 \cdot 32) - 3 \cdot 32 \\ &= 7 \cdot 46 - 10 \cdot 32 \end{aligned}$$

~~ANSWER~~

Thus, multiplying by  $-2$ ,

$$-4 = -14 \cdot 46 + 20 \cdot 32$$

$x = -14$   
 $y = 20$

answer

④ Why no  $x, y$  s.t.  $198x + 780y = 9$

There exist  $x, y$  like this iff

$9$  is in the ideal consisting of  
 $\mathbb{Z}$ -linear combinations of  $198$  and  $780$ .

This ideal is generated by the gcd.

So, is  $9$  a multiple of the  
gcd of  $198$  and  $780$ ? No.

$$780 = 3 \cdot 198 + 186$$

$$198 = 1 \cdot 186 + 12$$

$$186 = 15 \cdot 12 + \boxed{6}$$

$$12 = 2 \cdot 6 + 0$$

$$\therefore (198, 780) = 6$$

$9$  is not a multiple of  $6$ !

⑤ (i) Prove that the product of 3 consecutive integers is divisible by 6.

Look at  $n, n+1, n+2$ .

2 must be a factor of one of them

3 must be a factor of one of them.

Therefore 6 is a factor of their product.

Therefore 6 is a factor of their product.

(ii) Same for four consecutive integers  
2, 3, and 4 must be factors of  
 $n, n+1, n+2, n+3$ .

Therefore  $2 \cdot 3 \cdot 4 = 24$  is a factor  
of their product.

⑥ Prove that  $4 \mid (n^2 + 2)$  for any  $n$ .

Proof If  $n$  is odd, so is  $n^2 + 2$ , and 4 can't divide an odd number. So  $n$  is even, say  $n = 2k$  for some  $k \in \mathbb{Z}$ .

$$\text{Then } n^2 + 2 = 4k^2 + 2, \text{ but}$$

4 can't divide  $4k^2 + 2$ , since if it did, it would therefore divide 2 also!

⑦ Prove:  $x, y$  odd  $\Rightarrow x^2 + y^2$  even but not divisible by 4.

Proof:  $x, y$  odd  $\Rightarrow x^2, y^2$  odd  $\Rightarrow$   
 $x^2 + y^2$  even. For the second

part, write  $x = 2k+1, y = 2m+1$

for some  $k, m \in \mathbb{Z}$ . Then

$$\begin{aligned} x^2 + y^2 &= 4k^2 + 4k + 1 + 4m^2 + 4m + 1 \\ &= 4(k^2 + k + m^2 + m) + 2, \text{ which} \\ &\text{is not a multiple of 4.} \end{aligned}$$

⑧ Prove: There are no  $x, y$  such that  $x+y = 100$  and  $(x,y) = 3$ .

Proof If  $(x,y) = 3$ , then any

$\mathbb{Z}$ -linear combination  $ax+by$  is a multiple of 3. In particular, taking  $a=b=1$ ,  $x+y$  must be a multiple of 3, but 100 is not.

⑨ Prove: For  $g, l > 0$ ,  $\exists x, y$  s.t.  $(x,y) = g$ ,  $[x,y] = l$  iff  $g|l$

Proof " $\Rightarrow$ " Assume we have some  $x, y$  with  $(x,y) = g$ ,  $[x,y] = l$ . The set of  $\mathbb{Z}$ -linear combinations of  $x, y$  is the ideal  $(g)$ . The set of common multiples of  $x, y$  is the ideal  $(l)$ .

Every common multiple of  $x, y$  is also a linear combination of these, so  $(l) \subseteq (g)$ , which means  $g|l$ .

[Containment of ideals  $\leftrightarrow$  divisibility of generators, in opposite direction]

" $\Leftarrow$ " Assume  $g|l$ . We must produce  $x$  and  $y$  with the desired properties. Set  $x = g$ ,  $y = l$ .

⑩ Assume  $2^n+1 = xy$ ,  $x, y > 1$ ,  $n > 0$ .

Show that  $\forall a \in \mathbb{N}$ ,

$$2^a | x-1 \text{ iff } 2^a | y-1$$

Proof In terms of ideals, this is the same as showing

$$x-1 \in (2^a) \Leftrightarrow y-1 \in (2^a)$$

By symmetry, it's enough to show one direction only. So assume

$x-1 \in (2^a)$ . Since  $y > 1$ , it must be that  $n \geq a$ , which means  $2^n \in (2^a)$  also.

$$\text{Now, } x-1 \in (2^a) \Rightarrow xy - y \in (2^a)$$

$$\Rightarrow 2^n + 1 - y \in (2^a)$$

$$\Rightarrow 1 - y \in (2^a) \quad (\text{since } 2^n \in (2^a))$$

$$\Rightarrow y-1 \in (2^a)$$



- ⑪ Show every  $n > 0$  can be written uniquely as  $n = 2^m r$ , where  $r \geq 0$  and odd, positive.

Proof:  $n$  can be expressed uniquely as

$$n = \prod p_i^{a_i},$$

where the  $p_i$  run through all the primes and each  $a_i \geq 0$ , (with all but finitely many  $a_i = 0$ )

Thus  $p_1 = 2$ , and

$$\prod_{p_i \neq 2} p_i^{a_i} \text{ is odd.}$$

- ⑫ Prove that every positive integer ~~not~~ of the form  $3k+2$  has a prime factor of the same form.

Proof: Let  $n = 3k+2$ .  $n$  is positive, and it's not ~~odd~~ 1, so it has prime factors.

These are all of the form  $3m$ ,  $3m+1$ , or  $3m+2$  (since every integer is). None of them can have the form  $3m$ , since then 3 would divide  $3k+2$ , but it doesn't. If none of the prime factors had the form  $3m+2$ ,  $n$  would factor as

$$\begin{aligned} n &= (3k_1 + 1)^{a_1} (3k_2 + 1)^{a_2} \cdots (3k_r + 1)^{a_r} \\ &= 3(\text{---}) + 1, \text{ contradicting} \\ n &= 3k+2. \end{aligned}$$

- ⑬ Given  $p$  prime and  $a, b$   
 s.t.  $(a, p^2) = p$ ,  $(b, p^2) = p^2$   
 compute  $(ab, p^4)$  and  $(a+b, p^4)$

Sol'n The hypotheses imply

that  $p \mid a$  but  $p^2 \nmid a$

and  $p^2 \mid b$  but  $p^3 \nmid b$ .

Thus the exponent of  $p$  in  
 the prime factorization of  $ab$   
 is 3, so  $\boxed{(ab, p^4) = p^3}$ .

$p \mid a$  and  $p \mid b$ , so  $p \mid ab$ ,  
 but  $p^2 \nmid ab$  since if it did  
 it would also divide  $a^2(a+b) - b$ .

So  $\boxed{(a+b, p^4) = p}$

- ⑭ If  $(a, b) = c$  prove that  
 $(a^2, b^2) = c^2$ .

Proof: Write

$$a = \prod p_i^{a_i}$$

$$b = \prod p_i^{b_i}$$

where  $a_i, b_i \geq 0$ , all but finitely  
 many zero.

$$\text{Then } c = \prod p_i^{\min(a_i, b_i)}$$

$$\text{so } c^2 = \prod p_i^{2 \cdot \min(a_i, b_i)}$$

$$= \prod p_i^{\min(2a_i, 2b_i)}$$

$$= (a^2, b^2).$$

(15) Prove that any composite  $n$  has a prime factor  $\leq \sqrt{n}$ .

Proof: Write  $n = p_1 \cdot p_2 \cdots p_k$ ,

w/  $p_1, \dots, p_k$  primes. Since  $n$  is composite,  $k \geq 1$ .

Suppose for contradiction that each  $p_i > \sqrt{n}$ .

$$\text{Then } n = p_1 \cdots p_k > (\sqrt{n})^k > n.$$

impossible.

(16) Let  $S = \{1, \dots, n\}$ , and  $2^k$  be the largest power of 2 appearing in  $S$ .

Prove  $2^k$  does not divide any other number in  $S$ . Use this to prove

$$\sum_{i=1}^n \frac{1}{i} \notin \mathbb{Z}.$$

Proof Pick any  $x \in S$  such that  $2^k \mid x$ .

We show  $x = 2^k$ . By assumption there is some  $m$  s.t.  $m \cdot 2^k = x$ , with  $m \geq 1$ . If  $m > 1$  then  $x \geq 2^{k+1}$ ,

and since  $x \in S$ , so is  $2^{k+1}$ . But

$2^k$  was chosen to be the largest power of 2 in  $S$ . So  $m$  cannot be bigger

than 1. Hence  $m=1$ , so  $x = 2^k$ ,

i.e. the only member of  $S$  which divisible by  $2^k$  is  $2^k$  itself.

For the second part, put  $x = \sum_{i=1}^n \frac{1}{i}$ .

If  $x \in \mathbb{Z}$ , then so is  $N!x$ . But

$$N!x = N! + \frac{N!}{2} + \frac{N!}{3} + \cdots + \frac{N!}{2^k} + \cdots + \frac{N!}{N}$$

All terms are in  $\mathbb{Z}$  except  $\frac{N!}{2^k}$ , by the first part. Contradiction.

(17) If  $n > 0$  and  $2^n + 1$  is prime,  
then  $n$  is a power of 2.

(18) In the ring  $\mathbb{Z}[\sqrt{-11}]$ , factor  
15 in two ways,

Proof:

Notice that whenever  $k > 0$  is odd, we have

$$(x+1)(x^{k-1} - x^{k-2} + x^{k-3} - \dots - x + 1) \\ = x^k + 1$$

(need  $k$  odd to get everything to cancel correctly).

Now let  ~~$p$~~   $p = 2^n + 1$  be prime ( $n > 0$ ).

Factor  $n = 2^k \cdot m$  w/  $2 \nmid m$ , so  $m$  is odd

$$\text{Then } p = (2^{2^k})^m + 1 \text{ so } 2^{2^k} + 1 \mid p.$$

By the above observation, since  $p$  is prime  
and  $2^{2^k} + 1 > 1$ , we must have  $2^{2^k} + 1 = p$ ,

hence  $m=1$ , so  $n$  is a power of 2.

Sol'n:  $15 = 3 \cdot 5$

and  $15 = (2 + \sqrt{-11})(2 - \sqrt{-11})$