Chap 2.

Q2

(d). $\gcd(1769, 2378) = ?$

(1) $1769 = \underline{0} \cdot 2378 + \underline{1769}$

(2) $2378 = \underline{1}\, 1769 + \underline{609}$

(3) $1769 = 2 \cdot 609 + 551$

(4) $609 = 551 + 58$

(5) $551 = 9 \cdot 58 + \boxed{29}$

(6) $58 = 2 \cdot \boxed{29} + 0$

(1) $\Rightarrow \gcd(1769, 2378) = \gcd(2378, 1769)$

(2) $\Rightarrow \gcd(2378, 1769) = \gcd(1769, 609)$

$=$

$\vdots$

$= \dots = \gcd(58, 29) = \gcd(29, 0) = 29$

So $\gcd(1769, 2378) = 29$

Now to work backwards to find m, n such that

$$29 = m\,1769 + n\,2378$$

$(5) \Rightarrow \quad 29 = 551 - 9 \cdot 58$

$(4) \Rightarrow \quad = 551 - 9\,(609 - 551)$

$$= 10 \cdot 551 - 9 \cdot 609$$

$(3) \Rightarrow \quad = 10 \cdot (1769 - 2 \cdot 609) - 9 \cdot 609$

$$= 10 \cdot 1769 - 29 \cdot 609$$

$(2) \Rightarrow \quad = 10 \cdot 1769 - 29 \cdot (2378 - 1769)$

$$= \underbrace{-29}_{n} \cdot 2378 + \underbrace{39}_{m} \cdot 1769$$

$$29 = 1 \cdot 29 + 5 \cdot 0$$

$$= 1 \cdot 29 + 5 \cdot (58 - 2 \cdot 29)$$

$$= 5 \cdot 58 - 9 \cdot 29$$

$$= 5 \cdot 58 - 9\,(551 - 9 \cdot 58)$$

$$= -9 \cdot 551 + 86 \cdot 58$$

Q3. Prime factorization / canonical form of $n \in \mathbb{Z}$

$$n = \boxed{\prod_{i=1}^{r} p_i^{\alpha_i}}, \quad p_1 < p_2 < \dots < p_r$$

where p_i are distinct primes, $\alpha_i \geq 1$

Prove n is a square, i.e. $n = m^2$, for some $m \in \mathbb{Z}$, iff each α_i is even.

Suppose n is a square, i.e.

$n = m^2$, for some integer m.

Suppose m has canonical form

$$m = \prod_{i=1}^{s} q_i^{\beta_i},$$

for distinct primes q_i and $\beta_i \geq 1$.

$q_1 < q_2 < \dots < q_s$

$$\Rightarrow n = \left(\prod_{i=1}^{s} q_i^{\beta_i} \right)^2$$

$$= \boxed{\prod_{i=1}^{s} q_i^{2\beta_i}},$$

a canonical form for n.

F.T.A. says prime factorisations <u>are unique</u>

So $\square = \square$

$$\Rightarrow s = r,\ q_i = p_i,\ \alpha_i = 2\beta_i$$

$$\Rightarrow \alpha_i \text{ is even for all } i.$$

Conversely, suppose n has canonical form, with even exponents

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

where α_i are all even

i.e. $\alpha_i = 2\gamma_i$

$$= \prod_{i=1}^{r} p_i^{2\gamma_i}$$

$$= \Big(\underbrace{\prod_{i=1}^{r} p_i^{\gamma_i}}_{\in \mathbb{Z}}\Big)^2$$

So n is a square.

Q4 Conjecture.

If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$

then n is an m^{th}-power

iff $m \mid \alpha_i$, for each $1 \le i \le r$.

Proof follows similar lines 2nd m

Q8 For a pair of primes $p, q \geq 5$

$24 \mid p^2 - q^2$

Pf Idea. $24 = 2^3 \cdot 3$. We prove seperately that $2^3 \mid p^2 - q^2$ and $3 \mid p^2 - q^2$.

(Last week we proved: If $\gcd(x, y) = 1$ and $x \mid z$ & $y \mid z$ then $xy \mid z$).

Divisibility by 3??? Try the mod 6 idea from before.

$p = 6a + r \quad , \quad r = 1, 5$

$q = 6b + s \quad , \quad s = 1, 5$

maybe four cases to look at., or
lets use modular

$p \equiv r \pmod 6 \quad q \equiv s$

$p^2 \equiv r^2 \ , \ q^2 \equiv s^2 \qquad r, s = 1 \text{ or } 5$

$\equiv 1^2, 5^2 \qquad \equiv 1 \pmod 6$

$\equiv 1, 25 \qquad \ldots, -18, -12, -6, 0, 6, 12, 18, 36,$

$\equiv 1 \pmod 6$

$\Rightarrow \quad p^2 - q^2 \equiv 1 - 1 \equiv 0 \pmod 6$

$\Rightarrow \quad 6 \mid p^2 - q^2$

$\Rightarrow \quad 3 \mid p^2 - q^2$ divisibility by 3 ✓

Divisibility by 2??

(mod 6) only reveals one factor 2,

we need three.

Let's try another modulos (mod 2)

$p = 2a + 1$ since p, q primes ≥ 5

$q = 2b + 1$

$$p^2 - q^2 = (4a^2 + 4a + 1) - (4b^2 + 4b + 1)$$

$$= 4(a^2 + a - b^2 - b)$$

$$= 4(a^2 - b^2 + a - b)$$

$$= 4((a-b)(a+b) + (a-b))$$

$$= 4\underbrace{(a-b)(a+b+1)}_{\text{a factor of 2???}}.$$

Notice if a, b both even then a−b is even

" " odd " " " "

one odd, other even then a+b+1 is even

so in all cases (a−b)(a+b+1) is even

so is divisible by 2.

So p^2-q^2 is ~~divi~~ divisible by 8 ✓

Q? would working mod 4 work?

$$p = 4a + r \qquad q = 4b + s$$

$$\boxed{\begin{matrix} r = 1, 3 \\ s = 1, 3 \end{matrix}}$$

$$p^2 = 16a^2 + 8ar + r^2$$
$$q^2 = 16b^2 + 8bs + s^2$$

$$p^2 - q^2 = 16(a^2 - b^2) + 8(ar - bs) + \underbrace{r^2 - s^2}$$

$$1^2 - 1^2 = 0$$
$$1^2 - 3^2 = -8$$
$$3^2 - 1^2 = 8$$
$$3^2 - 3^2 = 0$$

$$\Rightarrow 8 \mid p^2 - q^2$$

<u>Q10</u> If $2^n - 1$ is prime then so is n.

"Mersenne primes" — primes of the form $\underbrace{2^p - 1}$

These are numbers that can be proved to be prime quicker than other typical

<u>Claim</u> $\boxed{(2^n-1) \text{ prime} \Rightarrow n \text{ prime}}$

<u>Pf</u>: Proving directly seems hard

Instead, we'll prove the <u>contrapositive</u>.

$(A \Rightarrow B) \equiv (\neg B) \Rightarrow (\neg A)$ an equivalent logical statement

The contrapositive is

$(n \text{ is composite}) \Rightarrow (2^n - 1 \text{ is composite})$

<u>Pf</u> Assume $\boxed{n \text{ is composite}}$

$\Rightarrow \quad n = \underline{\ a\ } \times \underline{\ b\ }$

for ~~a,b~~ $1 < a, b < n \qquad 2 \leq a < n$

$2^n - 1 = 2^{ab} - 1$

$= (2^a)^b - 1^b \quad , \quad 1^b = 1$

$$= (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1)$$

$$\Rightarrow 2^n - 1 = \underbrace{(2^a - 1)}_{\geq 3} \times \underbrace{(\quad '' \quad)}_{< 2^n - 1}$$

$$\Rightarrow \boxed{2^n - 1 \text{ is composite}},$$ since this is a non-trivial factorisation.

Common factorization:

$$\boxed{x^b - y^b} = (x-y)\left(x^{b-1} + x^{b-2}y + x^{b-3}y^2 + x^{b-4}y^3 + \dots + xy^{b-2} + y^{b-1}\right)$$

$(2^a)^b - 1^b$

$x = 2^a,\ y = 1$

$$= (x-y)\sum_{j=0}^{b-1} x^{b-1-j}\,y^j$$