Number Theory 2000

1. (i)
$$\left.\begin{aligned} 161 &= 1.98 + 63 \\ 98 &= 1.63 + 35 \\ 63 &= 1.35 + 28 \\ 35 &= 1.28 + 7 \\ 28 &= 4.7 + 0 \end{aligned}\right\}$$

$\gcd(98, 161) = 7$

Backtracking,

$$\begin{aligned} 7 &= 35 - 28 = 35 - (63 - 35) \\ &= 2.35 - 63 = 2(98 - 63) - 63 \\ &= 2.98 - 3.63 = 2.98 - 3(161 - 98) \\ &= 5.98 - 3.161 \end{aligned}$$

A solution of equation is $x = 5, y = -3$ $\left(\frac{161}{7} = 23, \frac{98}{7} = 14\right)$

General solution is $x = 5 + 23t,\ y = -3 - 14t,\ t \in \mathbb{Z}$

(ii) Suppose $d \mid m, n$. Then $d \mid \{(9n+4) - 9.n\}$ i.e. $d \mid 4$ so $d = 1, 2$ or 4

Now $n = 4k+3$, so n is odd. As $d \mid n$, d is odd, so must be 1

Hence 1 is the only (+ hence greatest) common divisor.

(iii) We have to prove that, for all n, $10^{n+1} + 8$ is divisible by 12

For $n = 1$, $10^{n+1} + 8 = 10^2 + 8 = 108$ which is divisible by 12, ie true for $n = 1$.

Assume true for $n = k$, ie $10^{k+1} + 8$ divisible by 12, so $10^{k+1} + 8 = 12K$ $(K \in \mathbb{Z})$

Then $10^{(k+1)+1} + 8 = 10.10^{k+1} + 8 = 10(12K - 8) + 8 = 12(10K - 9)$
so is divisible by 12, ie true for $n = k+1$

Hence, by induction, it is true for all $n \geq 1$.

2. (i) [Bookwork]

Suppose not. Let complete list be $p_1, \ldots, p_n$

Let $P = p_1 \ldots p_n$ and let $Q = 4P - 1$

As $Q > 1$, it has a prime factor p

Since Q odd, p odd, so p is of form $4k+1$ or $4k-1$

If all factors are "$4k+1$", so is Q (if $a, b \equiv 1 \pmod 4$, so is ab)

But $Q = 4P - 1$, so we must have at least one p of form $4k-1$

Since list complete, $p = p_i$, for some i, so $p_i \mid Q$

But $p_i \mid P$ so we have $p_i \mid (4P - Q)$ ie $p_i \mid 1$, a contradiction

Hence our assumption was false, so there are infinitely many primes of the form $4k-1$.

(ii) As $p \neq 3$, $p = 3k+1$ or $3k-1$

If $p = 3k+1$, $4p - 1 = 12k + 3$. Thus is divisible by 3, so not prime

If $p = 3k-1$, $4p + 1 = 12k - 3$. Thus is divisible by 3, so not prime

Thus, in any case, they cannot both be prime.

3(i)(a) True (Cf. is a theorem in the Unit)

Suppose $a \equiv b \pmod{m}$, so $a - b = km$, $k \in \mathbb{Z}$
and $d \mid m$, so $m = \ell d$ $\ell \in \mathbb{Z}$

Then $a - b = (k\ell)d$. As $(k\ell) \in \mathbb{Z}$, this means that $a \equiv b \pmod{d}$

(b) False (only true if d, m/d coprime)

Let $a = 2, b = 0, d = 2, m = 4$. Then $0 \equiv b \pmod 2$ and $a \equiv b \pmod{4/2}$

but $a \not\equiv b \pmod 4$.

(ii) [First we write each congruence as "$x \equiv a \pmod m$"]

$2x + 3 \equiv 1 \pmod 7 \iff 2x \equiv -2 \pmod 7 \iff x \equiv -1$, ie $x \equiv 6 \pmod 7$

$2x \equiv 7 \pmod{13} \iff 2x \equiv 20 \pmod{13}$ $(20 = 7 + 13)$
$\iff x \equiv 10 \pmod{13}$

Thus, the system is $x \equiv 1 \pmod 2$, $x \equiv 6 \pmod 7$, $x \equiv 10 \pmod{13}$

For mod 7, $x = 10, 23, 36, 49, \underline{62}$
mod 7: 3, 2, 1, 0, 6
} so $x \equiv 62 \pmod{7 \times 13 = 91}$

Thus, $x = 62, \underline{153}, \ldots$
mod 2: 0, 1
so $x \equiv 153 \pmod{182}$

It follows that the smallest positive solution is $\underline{153}$

4. (i) By Fermat, as 17 is prime $5^{16} \equiv 1 \pmod{17}$

Thus $5^{20} \equiv 5^{16} \cdot 5^4 \equiv 5^4 \equiv (5^2)^2 \equiv 8^2 \equiv 64 \equiv 13 \pmod{17}$ [$5^2 = 25 \equiv 8 \pmod{17}$]

Similarly, $3^{16} \equiv 1 \pmod{17}$, so

$$3^{20} \equiv 3^{16} \cdot 3^4 \equiv 3^4 \equiv 9^2 = 81 \equiv 13 \pmod{17}$$

Hence $5^{20} - 3^{20} \equiv 0 \pmod{17}$, ie $5^{20} - 3^{20}$ divisible by 17.

(ii) As 17 prime, Wilson's Theorem says $16! \equiv -1 \pmod{17}$

Thus, $16! + 1 \equiv 0 \pmod{17}$, ie $17 \mid (16! + 1)$.

If p is a prime less than 17, then $p \mid 16!$

If p also divides $16! + 1$, then it divides 1 (the difference)
This is false as p prime.

Thus 17 is smallest prime factor.

(iii) Since length is 22, 10 has order 22 mod 23, ie

$10^{22} \equiv 1 \pmod{23}$, but $10^k \not\equiv 1 \pmod{23}$ if $0 < k < 22$ (*)

(a) Let $b = 10^{11}$. Then $b^2 \equiv 10^{22} \equiv 1 \pmod{23}$

As 23 prime, $b \equiv 1$ or $b \equiv -1 \pmod{23}$ ($23 \mid (b-1)(b+1) \ldots$)

By (*), $b \neq 1$, so $b \equiv -1 \pmod{23}$.

(b) $3/23$ has digits in same cyclic order, but with a different start (& end)

Multiplying $1/23$ by 3, we see $3/23$ ends "39"

ie $3/23 = 0.\overline{\langle 130434782608695652173 9 \rangle}$

5 (i) (Bookwork)

$\phi(n)$ is the number of integers a, $1 \le a \le n$ with $\gcd(a,n)=1$

If $n=p^k$, the integers a with $\gcd(a,p^k) \neq 1$ are $a = bp$ $1 \le b \le p^{k-1}$

Thus $\phi(p^k) = p^k - p^{k-1} = p^k(1-1/p)$

Now suppose that $n = p_1^{k_1} \dots p_r^{k_r}$

As ϕ multiplicative $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_r^{k_r}) = p_1^{k_1}\left(1-\frac{1}{p_1}\right) \dots p_r^{k_r}\left(1-\frac{1}{p_r}\right)$

Collecting the "$p_i^{k_i}$" terms, $\phi(n) = p_1^{k_1} \dots p_r^{k_r} \prod_{p|n}(1-1/p) = n \prod_{p|n}(1-1/p)$.

(ii) (a) Let $n=p^2$, p prime. Then $\sigma(n) = \sigma(p^2) = 1+p+p^2$, so

$3n+\sigma(n) = 4p^2 + p + 1 \equiv 0 \pmod 4 \iff p+1 \equiv 0 \pmod 4 \iff p \equiv 3 \pmod 4$.

(b) Let $n=p^3$, p prime, Then $\sigma(n) = 1+p+p^2+p^3$

$3n+\sigma(n) = 4p^3+p^2+p+1 \equiv 0 \pmod 4 \iff p^2+p+1 \equiv 0 \pmod 4$

But $p^2+p = p(p+1)$ is always even, so p^2+p+1 is odd, so not $0 \pmod 4$

Thus $n=p^3$ is impossible.

(c) Let $n=pq$, p,q prime, $p<q$. Then $\sigma(n) = 1+p+q+pq$

$3n+\sigma(n) = 4pq+p+q+1 \equiv 0 \pmod 4 \iff p+q+1 \equiv 0 \pmod 4$

$q > p \ge 2$, so q odd so $p+q+1$ will be <u>odd</u> if p is odd

Thus $4 \mid (3n+\sigma(n)) \iff p=2$ and $2+q+1 \equiv 0 \pmod 4$, i.e. <u>$q \equiv 1 \pmod 4$</u>

6. (i) Discriminant is $7^2 - 4.3.3 = 13$

Thus, the equation has a solution $\Leftrightarrow \left(\frac{13}{23}\right) = 1$

$\left(\frac{13}{23}\right) = \left(\frac{23}{13}\right)$ [as $13 \equiv 1 \pmod 4$]

$= \left(\frac{10}{13}\right)$ [as $23 \equiv 10 \pmod{13}$]

Reasons not needed

$= \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = (-1)\left(\frac{13}{5}\right)$ [as $13 \equiv 5 \pmod 8$ & $5 \equiv 1 \pmod 4$]

$= (-1)\left(\frac{3}{5}\right) = (-1)\left(\frac{5}{3}\right) = (-1)\left(\frac{2}{3}\right) = 1$ [as $3 \equiv 3 \pmod 8$]

so we have a solution

(ii) $\left(\frac{94}{107}\right) = \left(\frac{2}{107}\right)\left(\frac{47}{107}\right)$ [$107 \equiv 3 \pmod 8$, $107 \equiv 47 \equiv 3 \pmod 4$]

$= (-1)\left(-\left(\frac{107}{47}\right)\right)$

$= \left(\frac{107}{47}\right) = \left(\frac{13}{43}\right)$ [$107 \equiv 13 \pmod{47}$]

$= \left(\frac{43}{13}\right) = \left(\frac{4}{13}\right) = 1$ [$13 \equiv 1 \pmod 4$, $4 = 2^2$]

(iii) Gauss Lemma: $(a/p) = (-1)^m$ where

m is the no. of integers in set $\{a.1, a.2, \ldots, a\frac{p-1}{2}\}$ which are congruent mod p to an integer in range $\frac{p+1}{2}, \ldots, p-1$.

Here $a = -2$, $p = 8k+1$ so $\frac{p-1}{2} = 4k$

Set is $\{-2, -4, -6, \ldots, -8k\}$ [$-\alpha \equiv p - \alpha \pmod p$]

$\equiv \{p-2, p-2.2, \ldots, p-4k.2\}$

$p - 2\alpha \geq \frac{p+1}{2} = 4k+1$ i.e. $8k+1-2\alpha \geq 4k+1$

$\Leftrightarrow 4k \geq 2\alpha \Leftrightarrow \alpha \leq 2k$

Thus $m = 2k$ here, so $(-2/p) = (-1)^{2k} = 1$.

7. (i) $37 = 3 \cdot 11 + 4$
$11 = 2 \cdot 4 + 3$
$4 = 1 \cdot 3 + 1$
$3 = 3 \cdot 1 + 0$

$\frac{37}{11} = [3, 2, 1, 3]$

$= [3, 2, 1, 2, 1]$ (convert Rac final "n" by "n-1, 1")

(ii) We have $p_k q_{k-1} - p_{k-1} q_k = (-1)^k$

Thus, if $d \mid p_k, q_k$, then $d \mid (p_k q_{k-1} - p_{k-1} q_k)$ i.e. $d \mid (-1)^k$

The only positive d is 1, so $\gcd(p_k, q_k) = 1$.

(iii) Let $x = [\langle 2, 3 \rangle]$

Then $x = [2, 3, \langle 2, 3 \rangle] = [2, 3, x] = 2 + \frac{1}{3 + \frac{1}{x}} = 2 + \frac{x}{3x+1} = \frac{7x+2}{3x+1}$

Thus $x(3x+1) = 7x+2$, i.e. $3x^2 - 6x - 2 = 0$

By formula, $x = \frac{6 \pm \sqrt{60}}{6} = \frac{3 + \sqrt{15}}{3}$ $\quad \sqrt{60} = 2\sqrt{15}$

Then $[1, 1, \langle 2, 3 \rangle] = [1, 1, x] = 1 + \frac{1}{1 + \frac{1}{x}} = 1 + \frac{x}{1+x} = \frac{2x+1}{x+1}$

$= \frac{2\left(\frac{3+\sqrt{15}}{3}\right) + 1}{\frac{3+\sqrt{15}}{3} + 1} = \frac{9 + 2\sqrt{15}}{6 + \sqrt{15}}$ (I think this would do

(optional bonus)

$= \frac{(9 + 2\sqrt{15})(6 - \sqrt{15})}{(6+\sqrt{15})(6-\sqrt{15})} = \frac{24 + 3\sqrt{15}}{21} = \frac{8 + \sqrt{15}}{7}$.

8. (i) $\sqrt{5} = 2 + (\sqrt{5}-2)$ $\quad [\sqrt{5}] = 2$

$\frac{1}{\sqrt{5}-2} = \frac{\sqrt{5}+2}{(\sqrt{5}-2)(\sqrt{5}+2)} = \frac{\sqrt{5}+2}{1} = 4 + (\sqrt{5}-2)$ $\quad [\sqrt{5}+2] = 4$

Same as previous residue!

Hence $\sqrt{5} = [2, \langle 4 \rangle]$

Cycle has length 1 (odd), so solutions from $2^{nd}, 4^{th}, \ldots$ convergents

p_k	1	2	9	38	161
a_k		2	4	4	4
q_k	0 "dummy"	1	4	17	72

So solutions are (9,4) and (161, 72).

(ii) (a) $368 = 2^4 . 23$ so not sum of 2 squares ($23 \equiv 3 \pmod 4$ occurs to odd power)

$= 4^2\{8.2 + 7\}$ so not sum of 3 squares

$370 = 2.5.37$ sum of 2 squares

$\neq 4^k(8k+7)$ so is sum of 3 squares

$372 = 2^2 . 3 . 31$ not sum of 2 squares (3 to odd power)

$= 4^1(8.11 + 5)$ so is sum of 3 squares.

(b) $370 = 10.37 = (3^2+1^2)(6^2+1^2)$ (smaller is easier!)

$= 19^2 + 3^2$ $\quad ((ab+cd)^2 + (bc-ad)^2)$