1985 Exam (381)

①(i) Prove by induction $1^3+2^3+\cdots+n^3 = \frac{1}{4}n^2(n+1)^2$

Let $P(n)$ be the statement $1^3+\cdots n^3 = \frac{1}{4}n^2(n+1)^2$

Then $P(1)$ holds.

Assume $P(k)$ holds; We show $P(k+1)$ holds:

$$1^3+\cdots(k+1)^3 = [1^3+\cdots+k^3] + (k+1)^3$$
$$= \tfrac{1}{4}k^2(k+1)^2 + (k+1)^3$$
$$= \tfrac{1}{4}(k+1)^2[k^2+4(k+1)]$$
$$= \tfrac{1}{4}(k+1)^2(k+2)^2 \quad \text{as required.}$$

Thus, by the principle of math indⁿ $P(n)$ holds $n\geq 1$

(ii) Use the Euclidean Algorithm to find $\gcd(221,391)$, and hence find integers x, y with $\gcd(221,391) = 221x - 391y$

$(221 = 0.391 + 221)$	$17 = 170 - 3.51$
$391 = 1.221 + 170$	$= 170 - 3.(221 - 1.170)$
$221 = 1.170 + 51$	$= 4.170 - 3.221$
$170 = 3.51 + 17$	$= 4.(391 - 1.221) - 3.221$
$51 = 3.17$	$= 4.391 - 7.221$

thus $x = -7$, $y = -4$ is a solution

(iii) The Lucas sequence $1,3,4,7\cdots$ is defined by $l_{n+2} = l_{n+1} + l_n$, $l_1 = 1$, $l_2 = 3$. Show $\gcd(l_n, l_{n+1}) = 1$ $n\geq 1$.

Proof by induction: true for $n=1$

Assume true $n=k$

$$\gcd(l_{k+1}, l_{k+2}) = \gcd(l_{k+1}, l_{k+1}+l_k)$$
$$= \gcd(l_{k+1}, l_k) \quad \text{as required}$$

(This is the lemma for the Euclidean Algorithm)

②(i) Prove there are infinitely many primes of the form 4k[+3]

Assume there are a finite no. $q_1\cdots q_n$

Let $N = (p_1\cdots p_n)^2 + 2 = 4k'+3$

N has an odd prime divisor q. Not all such q can be $(4k+1)$ type so $q = 4k''+3$. q can't be p_i since then $q \mid (p_1\cdots p_n)^2$ and $N \Rightarrow q \mid 2$ ✗.

(ii) If $p>5$ is prime prove p^2-1 or p^2+1 is div by 10

	p	p^2	p^2-1	p^2+1
	$10k+1$	$10k'+1$	$10k'$	
	$10k+3$	$10k'+9$	$10k'+8$	$10k''$
not prime	~~$10k+5$~~			
	$10k+7$	$10k'+9$	$10k'+8$	$10k''$
	$10k+9$	$10k'+1$	$10k'$	

In each case p^2-1 or p^2+1 is divisible by 10

---

③(i) Prove, using only the defn, that:

(a) $a \equiv b \pmod n \Rightarrow ka + c \equiv kb + c \pmod n$

$a - b = pn \Rightarrow ka + c - (kb + c) = k(a-b) = (kp)n$

$\Rightarrow$ desired result

(b) $ka \equiv kb \pmod n$, $\gcd(k,n) = 1$; then $a \equiv b \pmod n$

$ka - kb = pn \Rightarrow k(a-b) = pn$

$\Rightarrow k \mid pn \Rightarrow k \mid p$ Euclid's Lemma

Let $p = qk$ $\Rightarrow (a-b) = qn \Rightarrow a \equiv b \pmod n$

(ii) Solve $7x \equiv 6 \pmod{11}$ and $7x \equiv 4 \pmod{23}$

Find the smallest pos. odd integer satisfying both

$7x \equiv 6 \pmod{11}$	$7x \equiv 4 \pmod{23}$
$\Rightarrow 7x \equiv 28 \pmod{11}$	$\Rightarrow -16x \equiv 4 \pmod{23}$
$\Rightarrow x \equiv 4 \pmod{11}$	$\Rightarrow -4x \equiv 1 \equiv 24 \pmod{23}$
	$\Rightarrow x \equiv -6 \equiv 17 \pmod{23}$