SOLUTIONS TO HOMEWORK 3

1. (i) Note that $\phi(1000) = \phi(2^3)\phi(5^3) = 2^2 \cdot 5^2 \cdot 4 = 400$ and $(83, 1000) = 1$. Then by Euler's theorem, one finds that $83^{7601} = (83^{400})^{19} \cdot 83 \equiv 83 \pmod{1000}$. Thus the last three digits of 83^{7601} must be 083.

Observe next that $5^2 \equiv 25 \pmod{100}$, and $5(25) \equiv 25 \pmod{100}$, so that an obvious induction yields the conclusion that $5^k \equiv 25 \pmod{100}$ for each $k \geqslant 2$. Consequently, the last two digits of 5^{2025} are 25.

(ii) When $n \geqslant 0$, one has

$$2^{5n+4} + 7^{2n} \equiv 16 \cdot 32^n + 49^n \equiv 16 \cdot 15^n + 15^n \equiv 17 \cdot 15^n \equiv 0 \pmod{17}.$$

Thus 17 divides $2^{5n+4} + 7^{2n}$ for each $n \geqslant 0$.

2. (i) Fermat's Theorem shows that for each integer x one has that x^6 is congruent to one of 0 and 1 modulo 7. Thus, if we suppose that $x^3 \equiv 4 \pmod 7$, so that $x^6 \equiv 4^2 \equiv 2 \pmod 7$, then 2 must be congruent to one of 0 and 1 modulo 7. This gives a contradiction, and thus $x^3 \equiv 4 \pmod 7$ is insoluble. Next, if $x^3 - 4y^3 \equiv 0 \pmod 7$ is soluble with $y \not\equiv 0 \pmod 7$, then $y^{-1} \pmod 7$ exists, and so there exists a residue $z = xy^{-1} \pmod 7$ with $z^3 \equiv 4 \pmod 7$. This yields a contradiction which shows that the only solution of $x^3 \equiv 4y^3 \pmod 7$ is the trivial solution $x \equiv y \equiv 0 \pmod 7$. But if $x^3 - 4y^3 = 0$ were to have a non-zero integral solution, then by homogeneity one may suppose that a solution exists with $(x, y) = 1$, and in particular with $x \not\equiv 0 \pmod 7$ or $y \not\equiv 0 \pmod 7$. This contradicts our earlier deduction, whence the equation $x^3 - 4y^3 = 0$ has no solution in rational integers except $(x, y) = (0, 0)$.

Suppose now that $\sqrt[3]{4} \in \mathbb{Q}$. Then there exist $a, b \in \mathbb{Z}$ with $b > 0$ and $a/b = \sqrt[3]{4}$, and $a^3 - 4b^3 = 0$ is soluble in integers $(a, b) \neq (0, 0)$. This contradicts the conclusion of the previous paragraph, and thus $\sqrt[3]{4}$ is irrational.

(ii) Suppose that $x^3 - 4y^3 + 14z^3 = 0$ has a solution in integers other than $(x, y, z) = (0, 0, 0)$. By homogeneity we may suppose that one at least of x, y and z is not divisible by 7. But this equation is soluble only when $x^3 \equiv 4y^3 \pmod 7$, and this congruence has only the solution $x \equiv y \equiv 0 \pmod 7$. Thus $7 \nmid z$. Put $x_1 = x/7$ and $y_1 = y/7$, so that x_1 and y_1 are integers. Then making a substitution and dividing through by 7, we obtain $2z^3 + 7^2(x_1^3 - 4y_1^3) = 0$. Then $7|z$, contradicting our earlier deduction. This contradiction shows that the above equation possesses only the trivial solution.

3. (i) The integers 5, 19 and 3 are pairwise coprime and $5 \cdot 19 \cdot 3 = 285$. If $3x \equiv 2 \pmod 5$, $2x \equiv 3 \pmod{19}$ and $7x \equiv 5 \pmod 3$, then $x \equiv 4 \pmod 5$, $x \equiv 11 \pmod{19}$ and $x \equiv 2 \pmod 3$. We seek solutions to the congruences

$$(19 \cdot 3)y_1 \equiv 1 \pmod 5, \quad (3 \cdot 5)y_2 \equiv 1 \pmod{19}, \quad (5 \cdot 19)y_3 \equiv 1 \pmod 3,$$

so that $2y_1 \equiv 1 \pmod 5$, $15y_2 \equiv 1 \pmod{19}$, $2y_3 \equiv 1 \pmod 3$. We therefore deduce that $y_1 \equiv 3 \pmod 5$, $y_2 \equiv -5 \pmod{19}$, $y_3 \equiv 2 \pmod 3$. Thus, by the Chinese Remainder Theorem, the required solution is

$$x \equiv (19 \cdot 3) \cdot 3 \cdot 4 + (3 \cdot 5) \cdot (-5) \cdot 11 + (5 \cdot 19) \cdot 2 \cdot 2 = 239 \pmod{285}.$$

So a suitable integer is 239, and any integer of the form $239 + 285k$ ($k \in \mathbb{Z}$), satisfies the same property.

(ii) The integers 7, 23 and 9 are pairwise coprime and $7 \cdot 23 \cdot 9 = 1449$. If $3x \equiv 2 \pmod 7$, $5x \equiv 3 \pmod{23}$ and $7x \equiv 5 \pmod 9$, then $x \equiv 3 \pmod 7$, $x \equiv -4 \pmod{23}$ and $x \equiv 2 \pmod 9$. We seek solutions to the congruences

$$(23 \cdot 9)y_1 \equiv 1 \pmod 7, \quad (7 \cdot 9)y_2 \equiv 1 \pmod{23}, \quad (7 \cdot 23)y_3 \equiv 1 \pmod 9,$$

so that $4y_1 \equiv 1 \pmod 7$, $17y_2 \equiv 1 \pmod{23}$, $8y_3 \equiv 1 \pmod 9$. We therefore deduce that $y_1 \equiv 2 \pmod 7$, $y_2 \equiv -4 \pmod{23}$, $y_3 \equiv -1 \pmod 9$. Thus, by the Chinese Remainder Theorem, the required solution is

$$x \equiv (23 \cdot 9) \cdot 2 \cdot 3 + (7 \cdot 9) \cdot (-4) \cdot (-4) + (7 \cdot 23) \cdot (-1) \cdot 2 \equiv 1928 \equiv 479 \pmod{1449}.$$

So a suitable integer is 479, and any integer of the form $479 + 1449k$ ($k \in \mathbb{Z}$), satisfies the same property.

(iii) If the integer x satisfies $2x \equiv 5 \pmod{15}$ and $5x \equiv 7 \pmod{33}$, then in particular we have $2x \equiv 2 \pmod 3$ and $2x \equiv 1 \pmod 3$, whence $1 \equiv 2x \equiv 2 \pmod 3$, leading to a contradiction. Then there are no solutions to this pair of simultaneous congruences.

4. (i) Suppose that there are only finitely many primes of the shape $4k + 1$, say $p_1, \ldots, p_n$. Let $P = 2p_1p_2 \cdots p_n$, and put $Q = P^2 + 1$. Then Q is odd, and if $p|Q$, then $x^2 + 1 \equiv 0 \pmod p$ has the solution $x = P$. Then the prime divisors of Q are all congruent to 1 modulo 4. By construction, one has $(Q, p_i) = (P^2+1, p_i) = 1$ for each i, because $p_i|P$. Then none of the finite set of primes congruent to 1 modulo 4 divide Q. We have arrived at a contradiction, and this proves that there are infinitely many primes of the shape $4k + 1$.

(ii) Suppose that there are only finitely many primes of the shape $8k + 5$, say $p_1, \ldots, p_n$. Let $P = p_1p_2 \ldots p_n$, and put $Q = (2P)^2 + 1$. Then Q is odd, and if $p|Q$, then $x^2 + 1 \equiv 0 \pmod p$ has the solution $x = 2P$. Then the prime divisors of Q are congruent to 1 modulo 4. Since P is odd and $2 \nmid P$, one has $P^2 \equiv 1 \pmod 8$. Thus $4P^2 + 1 \equiv 5 \pmod 8$, and hence Q is divisible by some prime π not congruent to 1 modulo 8. But the primes dividing Q are congruent to 1 modulo 4, so the only possibility is that $\pi \equiv 5 \pmod 8$. Moreover, one has $(Q, p_i) = (4P^2+1, p_i) = 1$ for each i, because $p_i|P$. Then none of the finite set of primes congruent to 5 modulo 8 divide Q. This gives a contradiction, proving that there are infinitely many primes of the shape $8k + 5$.

5. (i) One has $(n, n + 1) = 1$, and hence any prime divisor π of $n + 1$ does not divide n. The desired conclusion follows on noting that $\pi \leqslant n + 1$.

(ii) By the binomial theorem, for each natural number n one has

$$q^n \geqslant 2^n = (1 + 1)^n \geqslant \binom{n}{1} + 1 = n + 1.$$

(iii) Suppose that p is the least prime not dividing n, and write $p-1=\pi_1^{a_1}\dots\pi_m^{a_m}$, where $\pi_1<\dots<\pi_m$ are prime numbers and $a_i\in\mathbb{N}$. We must have $\pi_i|n$ for each i, and moreover parts (ii) and (i), respectively, show that $\pi_i^n\geqslant n+1\geqslant p$. In particular, it follows that $a_i\leqslant n$ for each i, and hence $\pi_1^{a_1}\dots\pi_m^{a_m}|(\pi_1\dots\pi_m)^n$. Since also $\pi_1\dots\pi_m|n$, it follows that $\pi_1^{a_1}\dots\pi_m^{a_m}|n^n$, whence $(p-1)|n^n$.

(iv) Suppose that π is a prime number dividing n. Then since $(n,n^{n^n}-1)=1$, we see that π does not divide $n^{n^n}-1$. Then the only prime divisors of $n^{n^n}-1$ do not divide n. Let p be the least prime not dividing n. From part (iii) we have $(p-1)|n^n$, say $n^n=l(p-1)$. Then by Fermat's Little Theorem, since we have $(n,p)=1$, one finds that $n^{n^n}-1=(n^{p-1})^l-1\equiv 0\pmod{p}$, whence $p|(n^{n^n}-1)$. Thus, the least prime not dividing n is the smallest prime divisor of $n^{n^n}-1$.

(v) Now let p_k be the k-th smallest prime, and put $n=p_1p_2\dots p_k$. The smallest prime number not dividing n is p_{k+1}, and by part (iv) one sees that this is the smallest prime divisor of $n^{n^n}-1$.