SOLUTIONS TO HOMEWORK 3

1. (i) Note that $\phi(1000) = \phi(2^3)\phi(5^3) = 2^2 \cdot 5^2 \cdot 4 = 400$ (one can also see this directly by computing the number of odd integers a with $1 \leqslant a \leqslant 1000$ not divisible by 5). Then by Euler's theorem, on noting that $(79, 1000) = 1$, one finds that $79^{7201} = (79^{400})^{18} \cdot 79 \equiv 79 \pmod{1000}$. Thus the last three digits of 79^{7201} must be 079.

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^{2023} are 25.

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

$$2^{2n+5} - 3^{3n+2} \equiv 32 \cdot 4^n - 9 \cdot 27^n \equiv 32 \cdot 4^n - 9 \cdot 4^n \equiv 23 \cdot 4^n \equiv 0 \pmod{23}.$$

Thus 23 divides $2^{2n+5} - 3^{3n+2}$ for each $n \geqslant 0$.

2. (i) Since $0^3 \equiv 0 \pmod 7$ and $(\pm 1)^3 \equiv (\pm 2)^3 \equiv (\pm 3)^3 \equiv \pm 1 \pmod 7$, the congruence $x^3 \equiv 2 \pmod 7$ is insoluble. Next, if $x^3 - 2y^3 \equiv 0 \pmod 7$ 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 $z^3 \equiv 2 \pmod 7$. This yields a contradiction which shows that the only solution of $x^3 \equiv 2y^3 \pmod 7$ is the trivial solution $x \equiv y \equiv 0 \pmod 7$. But if $x^3 - 2y^3 = 0$ 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 $x^3 - 2y^3 = 0$ has no solution in rational integers except $(x, y) = (0, 0)$.

Suppose now that $\sqrt[3]{2} \in \mathbb{Q}$. Then there exist $a, b \in \mathbb{Z}$ with $b > 0$ and $a/b = \sqrt[3]{2}$, and $a^3 - 2b^3 = 0$ is soluble in integers $(a, b) \neq (0, 0)$. This contradicts the conclusion of the previous paragraph, and thus $\sqrt[3]{2}$ is irrational.

(ii) Suppose that $x^3 - 2y^3 + 7z^3 = 0$ 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 $x^3 \equiv 2y^3 \pmod 7$, 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 $z^3 + 7(x_1^3 - 2y_1^3) = 0$. Then $7|z$, contradicting our earlier deduction. This contradiction shows that the above equation possesses only the trivial solution.

3. (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 $n^{n^n}-1$.