SOLUTIONS TO HOMEWORK 4

1. (i) The integers 5, 23 and 3 are pairwise coprime and $5 \cdot 23 \cdot 3 = 345$. If $3x \equiv 2 \pmod 5$, $2x \equiv 3 \pmod{23}$ and $7x \equiv 5 \pmod 3$, then $x \equiv 4 \pmod 5$, $x \equiv 13 \pmod{23}$ and $x \equiv 2 \pmod 3$. We seek solutions to the congruences

$$(23 \cdot 3)y_1 \equiv 1 \pmod 5, \quad (3 \cdot 5)y_2 \equiv 1 \pmod{23}, \quad (5 \cdot 23)y_3 \equiv 1 \pmod 3,$$

so that $4y_1 \equiv 1 \pmod 5$, $15y_2 \equiv 1 \pmod{23}$, $y_3 \equiv 1 \pmod 3$. We therefore deduce that $y_1 \equiv -1 \pmod 5$, $y_2 \equiv -3 \pmod{23}$, $y_3 \equiv 1 \pmod 3$. Thus, by the Chinese Remainder Theorem, the required solution is

$$x \equiv (23 \cdot 3) \cdot (-1) \cdot 4 + (3 \cdot 5) \cdot (-3) \cdot 13 + (5 \cdot 23) \cdot 1 \cdot 2 = -631 \equiv 59 \pmod{345}.$$

So a suitable integer is 59, and any integer of the form $59 + 345k$ ($k \in \mathbb{Z}$), satisfies the same property.

(ii) The integers 7, 19 and 9 are pairwise coprime and $7 \cdot 19 \cdot 9 = 1197$. If $3x \equiv 2 \pmod 7$, $5x \equiv 3 \pmod{19}$ and $7x \equiv 5 \pmod 9$, then $x \equiv 3 \pmod 7$, $x \equiv -7 \pmod{19}$ and $x \equiv 2 \pmod 9$. We seek solutions to the congruences

$$(19 \cdot 9)y_1 \equiv 1 \pmod 7, \quad (7 \cdot 9)y_2 \equiv 1 \pmod{19}, \quad (7 \cdot 19)y_3 \equiv 1 \pmod 9,$$

so that $3y_1 \equiv 1 \pmod 7$, $6y_2 \equiv 1 \pmod{19}$, $7y_3 \equiv 1 \pmod 9$. We therefore deduce that $y_1 \equiv 5 \pmod 7$, $y_2 \equiv -3 \pmod{19}$, $y_3 \equiv 4 \pmod 9$. Thus, by the Chinese Remainder Theorem, the required solution is

$$x \equiv (19 \cdot 9) \cdot 5 \cdot 3 + (7 \cdot 9) \cdot (-3) \cdot (-7) + (7 \cdot 19) \cdot 4 \cdot 2 \equiv 164 \pmod{1197}.$$

So a suitable integer is 164, and any integer of the form $164 + 1197k$ ($k \in \mathbb{Z}$), satisfies the same property.

(iii) If the integer x satisfies $2x \equiv 7 \pmod{15}$ and $5x \equiv 17 \pmod{33}$, then in particular we have $2x \equiv 7 \pmod 3$ and $5x \equiv 17 \pmod 3$, whence $1 \equiv 2x \equiv 2 \pmod 3$, leading to a contradiction. Then there are no solutions to this pair of simultaneous congruences.

2. (i) By inspection (or using the theorem from class that $((p-1)/2)!^2 \equiv -1 \pmod p$ when $p \equiv 1 \pmod 4$), one finds that $2^2 \equiv -1 \pmod 5$ and $5^2 \equiv -1 \pmod{13}$. It therefore follows that whenever $x \equiv 2 \pmod 5$ and $x \equiv 5 \pmod{13}$, then $x^2 \equiv -1 \pmod{65}$. But a solution of the congruence $13y_1 \equiv 1 \pmod 5$ is given by $y_1 = 2$, and a solution of the congruence $5y_2 \equiv 1 \pmod{13}$ is given by $y_2 = 8$. Then since $65 = 5 \cdot 13$, it follows from the Chinese Remainder Theorem that a solution of the desired type is

$$x = 13 \cdot 2 \cdot 2 + 5 \cdot 8 \cdot 5 = 252 \equiv -8 \pmod{65}.$$

(ii) The congruence $x^2 \equiv -1 \pmod 5$ has the 2 solutions $x \equiv \pm 2 \pmod 5$, and the congruence $x^2 \equiv -1 \pmod{13}$ has the 2 solutions $x \equiv \pm 5 \pmod{13}$. Then, by the Chinese Remainder Theorem, the congruence $x^2 \equiv -1 \pmod{65}$ has $2 \cdot 2 = 4$ solutions modulo 65.

3. (i) By Fermat's Little Theorem, for all integers a one has $a^p \equiv a \pmod{p}$, and hence $a^p - a + 1 \equiv 1 \pmod{p}$. Thus we see that $x^p - x + 1 \equiv 0 \pmod{p}$ has no integral solution.
(ii) If $(x, 40) = d$, then $d|(x^{16} - x)$. Consequently, if $x^{16} - x + 3 \equiv 0 \pmod{40}$, we see that $x^{16} - x + 3 \equiv 0 \pmod{d}$, and hence $d|3$. But $d|40$ and $(40, 3) = 1$, and so $d = 1$. Observe next that $\varphi(40) = \varphi(8)\varphi(5) = 4 \cdot 4 = 16$. Thus, when $(a, 40) = 1$, it follows from Euler's theorem that $a^{16} \equiv 1 \pmod{40}$. In such circumstances, it follows that $a^{16} - a + 3 \equiv 4 - a \pmod{40}$. Then if $(x, 40) = 1$, we have $x^{16} - x + 3 \equiv 0 \pmod{40}$ if and only if $x \equiv 4 \pmod{40}$, yet $(4, 40) \neq 1$, so we arrrive at a contradiction. Hence, the equation $x^{16} - x + 3 \equiv 0 \pmod{40}$ has no solutions.

4. One has $1729 = 7 \cdot 13 \cdot 19$. By Fermat's Little Theorem, whenever $(a, 1729) = 1$, one has $a^6 \equiv 1 \pmod{7}$ because $(a, 7) = 1$, and $a^{12} \equiv 1 \pmod{13}$ because $(a, 13) = 1$, and $a^{18} \equiv 1 \pmod{19}$ because $(a, 19) = 1$. Hence, for all integers a with $(a, 1729) = 1$ one has

$$\begin{aligned} a^{1728} &= (a^6)^{288} \equiv 1 \pmod{7}, \\ a^{1728} &= (a^{12})^{144} \equiv 1 \pmod{13}, \\ a^{1728} &= (a^{18})^{96} \equiv 1 \pmod{19}. \end{aligned}$$

Thus we conclude that $a^{1728} \equiv 1 \pmod{1729}$, since $1729 = 7 \cdot 13 \cdot 19$.

5. (i) Suppose next 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 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 $8k + 5$.