# MATH453M Homework Solutions Week2

Nick Inglis
ninglis@math.purdue.edu

**1.3.5** The residue classes mod 3 are $0, \pm 1$ with $0^2 \equiv 0 \pmod 3$ and $(\pm 1)^2 \equiv 1 \pmod 3$. The residue classes mod 5 are $0, \pm 1, \pm 2$ with $0^2 \equiv 0 \pmod 5$, $(\pm 1)^2 \equiv 1 \pmod 5$ and $(\pm 2)^2 \equiv 4 \pmod 5$.

**1.3.8** $3^4 = 81 \equiv 1 \pmod{10}$ so $3^{400} = (3^4)^{100} \equiv 1 \pmod{10}$ so the last digit of $3^{400}$ is 1. To determine the last 2 digits we work mod 100, and start by working mod 4 and mod 25. Now $3^2 = 9 \equiv 1 \pmod 4$ also $3^4 \equiv 6 \pmod{25}$ so $3^8 \equiv 36 \equiv 11 \pmod{25}$, $3^{12} \equiv 66 \equiv -9 \pmod{25}$, $3^{16} \equiv -54 \equiv -4 \pmod{25}$ and $3^{20} \equiv -24 \equiv 1 \pmod{25}$. We have $3^{20} \equiv 1 \pmod 4$ and $3^{20} \equiv 1 \pmod{25}$ so, by the Chinese Remainder Theorem, $3^{20} \equiv 1 \pmod{100}$. Therefore $3^{400} = (3^{20})^{20} \equiv 1 \pmod{100}$ so the last two digits of $3^{400}$ are 01.

Now $7^4 = 2401 \equiv 1 \pmod{10}$ so $7^{96} = (7^4)^{24} \equiv 1 \pmod{10}$. Therefore $7^{99} \equiv 7^3 = 343 \equiv 3 \pmod{10}$ so the last digit is of $7^{99}$ is 3.

**1.3.16** $p$ is prime and $p \neq 3$ so $p \equiv \pm 1 \pmod 3$. Therefore $p^2 \equiv 1 \pmod 3$ and so $p^2 + 2 \equiv 3 \equiv 0 \pmod 3$. Thus 3 divides $p^2 + 2$ and $p^2 + 2 > 3$ so $p^2 + 2$ is composite.

**1.3.20 c** $243x + 17 \equiv 101 \pmod{725} \iff 243x \equiv 84 \pmod{725}$. Now

$$
\begin{aligned}
725 &= 2.243 + 239 \qquad & 1 &= 4 - 3 = 4 - (239 - 59.4) \\
243 &= 1.239 + 4 & &= 60.4 - 239 = 60(243 - 239) - 239 \\
239 &= 59.4 + 3 & &= 60.243 - 61.239 = 60.243 - 61(725 - 2.243) \\
4 &= 1.3 + 1 & &= 182.243 - 61.725
\end{aligned}
$$

Thus $\gcd(725, 243) = 1$ and $182.243 \equiv 1 \pmod{725}$ so $x \equiv 182.84 = 15288 \equiv 63 \pmod{725}$.

**1.3.20 g** Now $\gcd(35, 15) = 5$ and 5 divides 25 so $15x \equiv 25 \pmod{35} \iff 3x \equiv 5 \pmod 7$. We have $7 = 2.3 + 1$ so that $(-2).3 \equiv 1 \pmod 7$. Therefore $x \equiv (-2)5 \equiv -10 \equiv -3 \pmod 7$.

**1.3.20 h** Again $\gcd(35, 15) = 5$ but 5 does not divide 24 so there is no solution.

**1.3.21 c** We want to solve $x \equiv b_i \pmod{m_i}$ with $(b_1, m_1) = (3, 4)$, $(b_2, m_2) = (4, 5)$ and $(b_3, m_3) = (3, 7)$. Let $N = 4.5.7 = 140$ and let $n_i = N/m_i$. If we solve $n_i x_i \equiv b_i \pmod{m_i}$ then $x \equiv n_1 x_1 + n_2 x_2 + n_3 x_3 \pmod N$. Now $n_1 = 35 \equiv 3 \pmod 4$ so $3x_1 \equiv n_1 x_1 \equiv 3 \pmod 4 \iff x_1 \equiv 1 \pmod 4$.

And $n_2 = 28 \equiv -2 \pmod 5$ so $(-2)x_2 \equiv n_2 x_2 \equiv 4 \pmod 5 \iff x_2 \equiv -2 \pmod 5$.
Finally $n_3 = 20 \equiv -1 \pmod 7$ so $-x_3 \equiv n_3 x_3 \equiv 3 \pmod 7 \iff x_3 \equiv -3 \pmod 7$.
Therefore $x \equiv 35.1 + 28(-2) + 20(-3) = -81 \equiv 59 \pmod{140}$.

**1.3.21 d** Using the Chinese Remainder Theorem and $140 = 4.5.7$ we have $19x \equiv 1 \pmod{140}$ if and only $19x \equiv 1 \pmod{m_i}$ for $m_i = 4$, 5 and 7. Now $19 \equiv -1 \pmod 4$ so $-x \equiv 19x \equiv 1 \pmod 4 \iff x \equiv -1 \equiv 3 \pmod 4$. Similarly $19 \equiv -1 \pmod 5$ so $-x \equiv 19x \equiv 1 \pmod 5 \iff x \equiv -1 \equiv 4 \pmod 5$. Finally $19 \equiv -2 \pmod 7$ has multiplicative inverse $3 \pmod 7$ so $-2x \equiv 19x \equiv 1 \pmod 7 \iff x \equiv 3 \pmod 7$. Thus this problem is the same as 1.3.21 c and again has solution $x \equiv 59 \pmod{140}$.

[Note that a quicker solution would be to apply Euclid's algorithm directly.]

**1.3.21 f** We use Theorem 3.8. Here we have $x \equiv b_i \pmod{m_i}$ with $(b_1, m_1) = (4, 105)$ and $(b_2, m_2) = (29, 80)$. Now

$$\begin{aligned} 105 &= 1.80 + 25 \\ 80 &= 3.25 + 5 \\ 25 &= 5.5 \end{aligned} \qquad\qquad \begin{aligned} 5 &= 80 - 3.25 = 80 - 3(105 - 80) \\ &= 4.80 - 3.105 \\ &= a_1 m_1 + a_2 m_2 \end{aligned}$$

with $a_1 = -3$ and $a_2 = 4$. Thus $d = \gcd(105, 80) = 5$ and $b_1 - b_2 = 5 - 29 = -25 = (-5)5 = cd$ with $c = -5$ so there is a solution and the general form is

$$\begin{aligned} x &\equiv c a_2 m_2 + b_2 \pmod{m_1 m_2 / d} \\ &\equiv (-5)4.80 + 29 \equiv -1600 + 29 \equiv 109 \pmod{1680} \end{aligned}$$

**1.3.28** What are the possible residue classes mod 6 for a prime $p > 3$? Not $0, \pm 2$ since $p$ is odd and not 3 since 3 does not divide $p$, so $p \equiv \pm 1 \pmod 6$. Suppose that there are only finitely many primes $p_1, p_2, \ldots, p_k$ congruent to $-1$ mod 6. Let $N = 6p_1 p_2 \ldots p_k - 1$. Then $N \equiv -1 \pmod 6$ so 2 and 3 do not divide $N$. Also $N \equiv -1 \pmod{p_i}$ so $p_i$ does not divide $N$ for $1 \leqslant i \leqslant k$. Therefore $N$ must be a product of other primes, each of which is congruent to 1 mod 6. Hence $N \equiv 1 \pmod 6$ which contradicts the definition of $N$. Therefore there are infinitely many primes congruent to $-1$ mod 6.

**1.3.29 a** We have

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p \equiv x^p + y^p \pmod p$$

since $p$ divides $\binom{p}{k}$ for $1 \leqslant k < p$.

**1.3.29 b** Let $q = p^n$. We use induction on $n$. The result is true for $n = 1$ by part a, so suppose that $n > 1$ and that the result is true for smaller values of $n$. Then

$$\begin{aligned} (x+y)^{p^n} &= \left((x+y)^{p^{n-1}}\right)^p \equiv \left(x^{p^{n-1}} + y^{p^{n-1}}\right)^p \pmod p \qquad \text{since true for } n-1 \\ &\equiv \left(x^{p^{n-1}}\right)^p + \left(y^{p^{n-1}}\right)^p = x^{p^n} + y^{p^n} \pmod p \end{aligned}$$