AC

M3P14 Elementary Number Theory
Sheet2: Solutions.

(1) We have to solve

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 1 \mod 4 \end{cases}$$

By the Chinese remainder theorem the problem has a unique solution $\mod 3 \cdot 5 \cdot 4 = 60$. Let us first solve

$$\begin{cases} y \equiv 2 \mod 3 \\ y \equiv 3 \mod 5 \end{cases}$$

The solution is of the form $y \equiv 2 + 3u = 3 + 5v \mod 15$ where $3u - 5v = 1$; hence $(u, v) = (2, 1)$ will do; this gives $y \equiv 8 \mod 15$. We now solve

$$\begin{cases} x \equiv 8 \mod 15 \\ x \equiv 1 \mod 4 \end{cases}$$

The solution is of the form $x \equiv 8 + 15u = 1 + 4v \mod 60$ where $4v - 15u = 7$; here $(u, v) = (3, 13)$ will do; this gives the (unique) solution

$$x \equiv 53 \mod 60.$$

(3) We proceed by repeated squaring: first of all

$$9990 = 8192 + 1024 + 512 + 256 + 4 + 2$$

So:

$$\begin{aligned}
2^2 &= 4 \\
2^4 &= 16 \\
2^8 &= 256 \\
2^{16} &= 256^2 \equiv 5590 && \mod 9991 \\
2^{32} &= 5590^2 \equiv 6243 && \mod 9991 \\
2^{64} &= 6243^2 \equiv 158 && \mod 9991 \\
2^{128} &= 158^2 \equiv 4982 && \mod 9991 \\
2^{256} &= 4982^2 \equiv 2680 && \mod 9991 \\
2^{512} &= 2680^2 \equiv 8862 && \mod 9991 \\
2^{1024} &= 8862^2 \equiv 5784 && \mod 9991 \\
2^{2048} &= 5784^2 \equiv 4788 && \mod 9991 \\
2^{4096} &= 4788^2 \equiv 5590 && \mod 9991 \\
2^{8192} &= 5590^2 \equiv 6243 && \mod 9991.
\end{aligned}$$

Finally:

$$
\begin{aligned}
2^{9990} = 6243 \times 5784 \times 8862 \times 2680 \times 16 \times 4 \equiv \\
2038 \times 8862 \times 2680 \times 16 \times 4 \equiv \\
7019 \times 2680 \times 16 \times 4 \equiv 7858 \times 64 = 3362.
\end{aligned}
$$

From this it is clear that 9991 is not prime.

(4) **Comment.** I admit this is a very large calculation.

(a) We solve for x: $x^{113} \equiv 347 \mod 463$; we need a pocket calculator to do this. According to the general theory we can do this if $\mathrm{hcf}(347, 463) = \mathrm{hcf}(113, \varphi(463)) = 1$; now 463 is prime so $\varphi(463) = 462$; 113 is also prime and it does not divide 462, hence indeed $\mathrm{hcf}(113, 462) = 1$. Next we need **positive** integers y, z such that

$$113y - 462z = 1$$

The Euclidean algorithm:

$$
\begin{aligned}
462 &= 4 \times 113 + 10 \\
113 &= 11 \times 10 + 3 \\
10 &= 3 \times 3 + 1
\end{aligned}
$$

gives

$$
\begin{aligned}
1 = 10 - 3 \times 3 = 10 - 3 \times (113 - 11 \times 10) = -3 \times 113 + 34 \times 10 = \\
-3 \times 113 + 34 \times (462 - 4 \times 113) = 34 \times 462 - 139 \times 113.
\end{aligned}
$$

This gives integers $(y, z) = (-139, -34)$ with $113y - 462z = 1$ but they are not positive. The required positive solution is $(y, z) = (-139 + 462, -34 + 113) = (323, 79)$; to summarise, we found that

$$113 \times 323 - 462 \times 79 = 1$$

(check!). The answer to the question is

$$x \equiv 347^{323} \mod 463.$$

We calculate this with the method of repeated squaring:

$$323 = 256 + 67 = 256 + 64 + 2 + 1$$

and

$$
\begin{aligned}
347^2 &= 120,409 \equiv 29 \mod 463 \\
347^4 &\equiv 29^2 = 841 \equiv 378 \mod 463 \\
347^8 &\equiv 378^2 = 142,884 \equiv 280 \mod 463 \\
347^{16} &\equiv 280^2 = 78,400 \equiv 153 \mod 463 \\
347^{32} &\equiv 153^2 = 23,409 \equiv 259 \mod 463 \\
347^{64} &\equiv 259^2 = 67,081 \equiv 409 \mod 463 \\
347^{128} &\equiv 409^2 = 167,281 \equiv 138 \mod 463 \\
347^{256} &\equiv 138^2 = 19,044 \equiv 61 \mod 463.
\end{aligned}
$$

Finally

$$x \equiv 61 \times 409 \times 29 \times 347 \equiv 37 \mod 463.$$

(b) Similar. I just sketch the answer. First we need to check that $\mathrm{hcf}(b, m) = \mathrm{hcf}(275, 588) = 1$, which you can do e.g. running the Euclidean algorithm. Then you calculate $\varphi(588) = 168$ and

$$257y - 168z = 1$$

for $(y, z) = (11, 18)$ so $x \equiv 139^{11} \mod 588$. We compile our usual table:

$$139^2 \equiv 505 \mod 588$$
$$139^4 \equiv 421 \mod 588$$
$$139^8 \equiv 253 \mod 588$$

and $x \equiv 139^{11} \equiv 253 \times 505 \times 139 \equiv 559 \mod 588$.

(5) (a) This was proved in class but here is a slightly different proof. First of all a solution exists: if

$$ky - \varphi(m)z = 1$$

then $a = b^y$ is a k-th root of b. To see that there is only one solution we just need to show that the equation

$$x^k \equiv 1 \mod m$$

has as unique solution $x = 1$ (why?). But this is obvious: the order of x must divide both k (from the equation) and $\varphi(m)$ (the order of the group $(\mathbb{Z}/m\mathbb{Z})^\times$ where x lives) hence the order of x must be 1.

(b) (OK I admit this part of the question is rather tough.) Here we assume $\mathrm{hcf}\big(k, \varphi(m)\big) > 1$. It is enough to show that the equation

$$x^k \equiv 1 \mod m \tag{1}$$

always has at least 2 solutions (why?). We may assume that $k = q$ is prime (why?). Let $m = \prod p_i^{a_i}$ be the prime decomposition of m, then

$$\varphi(m) = \prod p_i^{a_i - 1}(p_i - 1)$$

Necessarily $q | p_i(p_i - 1)$ for some i and then it is enough to show that Equation (1) has at least two solutions mod $p_i^{a_i}$ (why?). So all I have to do is to produce an element $\gamma \not\equiv 1 \mod p_i^{a_i}$ that has order q in $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$. It is easy to show that γ exists if $a_i = 1$ (why?) so I will from now on assume that $a_i \geq 2$. There are two cases: (i) $q = p_i$ and (ii) $q | p_i - 1$; I treat them separately:

(i) Assume $q = p_i$. Note that we have surjective group homomorphism

$$f \colon (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times \to (\mathbb{Z}/p_i\mathbb{Z})^\times$$

with kernel a group K of order $p_i^{a_i - 1}$ (Lagrange). Consider now $1 + p_i \in K$; this element has order p_i^b for some $1 \leq b \leq p_i - 1$ and I can take $\gamma = (1 + p_i)^{q^{b-1}}$.

(ii) Assume now that $q | p_i - 1$. Let g be a primitive root modulo p and let $\tilde{g} \in (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ an element which maps to g under the homomorphism f. Now

$\tilde{g}$ has order $p_i^b(p_i-1)$ for some b (why?) and then $(\tilde{g})^{p_i^b}$ necessarily has order $p_i - 1$. In this case I can take

$$\gamma = (\tilde{g})^{p_i^b \frac{p_i-1}{q}}.$$

(c) It should not have been difficult for you to guess that the number of solutions is $\mathrm{hcf}(k, p-1)$ (assuming that at least one solution exists).

(6) (a) This is taked directly from the notes!

Claim. If m is square-free, then

$$a^{z\varphi(m)+1} \equiv a \mod m$$

for all a. Indeed write $m = p_1 p_2 \cdots p_k$ with p_i distinct primes; then

$$\begin{cases} a^{\varphi(m)} = a^{(p_1-1)(p_2-1)\cdots(p_k-1)} & \equiv 1 \mod p_i \quad \text{if } p_i \not| a \\ & \equiv 0 \quad \text{if } p_i \not| a \end{cases}$$

and the claim follows from the Chinese remainder theorem.

Using the claim:

$$(b^y)^k = b^{ky} = b^{z\varphi(m)+1} \equiv b \mod m.$$

(b) Here $(k, \varphi(m)) = (5, 6) = 1$, $(y, z) = (5, 4)$ and $b^y = 6^5 \equiv 0 \mod 9$.

(8) This is a very easy question

(a) If $ab \equiv 1 \mod m$, then $y \mapsto by$ is the inverse of $x \mapsto ax$.

(b) Obvious: by part (a) $S = \{ax \mid x \in S\}$.

(c) Taking products immedialy shows $P = a^{\varphi(m)}P$ and dividing both sides by P (why is this possible?) we get $a^{\varphi(m)} \equiv 1 \mod m$.

(10) The functions d, σ are multiplicative; indeed

$$d(n) = \sum_{d|n} 1 = \mathbf{1} * \mathbf{1}$$
$$\sigma(n) = \sum_{d|n} d = I * \mathbf{1}$$

and convolution of multiplicative functions is multiplicative (you can quote this without proof because it was stated in the lectures). If p is prime $d(p^k) = k+1$ and

$$\sigma(p^k) = 1 + p + p^2 + \cdots p^k = \frac{p^{k+1}-1}{p-1}.$$

(11)(a) These should have been easy:

$$\sum_{1 \le n \le x} \frac{\log n}{n} = \text{const} + O\Big(\frac{\log x}{x}\Big) + \int_1^x \frac{\log u}{u} du$$

and similarly for $\sum \frac{1}{n \log n}$.

(b) First you should draw a picture of integer points under a hyperbola, as we did in class, to persuade yourself that

$$\sum_{n\le x}\frac{d(n)}{n}=\sum_{n\le x}\sum_{d|n}\frac{1}{n}=\sum_{n\le x}\sum_{m\le x/n}\frac{1}{mn}.$$

This was the hard part. If you see this, then the rest is easy:

$$\begin{aligned}\sum_{n\le x}\frac{1}{n}\sum_{m\le x/n}\frac{1}{m}&=\sum_{n\le x}\frac{1}{n}\Big(\gamma+O\Big(\frac{n}{x}\Big)+\log\frac{x}{n}\Big)=\\&=\gamma\log x+O(1)+\sum_{n\le x}O\Big(\frac{1}{x}\Big)+\sum_{n\le x}\frac{1}{n}(\log x-\log n)=\\&=\gamma\log x+O(1)+\log x\Big(\sum_{n\le x}\frac{1}{n}\Big)-\sum_{n\le x}\frac{\log n}{n}=\\&=\frac{1}{2}\log^2 x+2\gamma\log x+O(1).\end{aligned}$$