Topics: Structure of integers mod m, primes, RSA.

3.1. Let p be a prime number and let m be an integer such that $m \mid (p-1)$. Prove that the group $(\mathbf{Z}/p\mathbf{Z})^\times$ has an element of order m.

Solution. We know that primitive roots modulo p exist; let g be one of them, so that g has order $p-1$.

Write $p-1 = mq$ and let $a = g^q$. Then $a^m = g^{mq} = g^{p-1} = 1$. Also, if $a^j = 1$ for some $j < m$, then $g^{jq} = 1$ for $jq < mq = p-1$, contradicting the fact that the order of g is $p-1$. □

3.2. Prove the following formula for the Euler phi function:

$$\phi(m) = m \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right),$$

where $p_1, \dots, p_r$ are the distinct prime factors of m.

Solution. Write $m = p_1^{e_1} \dots p_r^{e_r}$. We have seen that

$$\phi(m) = \phi(p_1^{e_1}) \dots \phi(p_r^{e_r})$$

and

$$\phi(p^e) = p^{e-1}(p-1) = p^e \left(1 - \frac{1}{p}\right).$$

The desired formula follows from these two equations. □

3.3. Prove that if $a \mid b$ then $\phi(a) \mid \phi(b)$.

Solution. First consider the special case $a = p^f$, $b = p^e$ for a prime number p. Since $a \mid b$ we have $f \leqslant e$. Also

$$\phi(a) = \phi(p^f) = p^{f-1}(p-1) \quad \text{and} \quad \phi(b) = \phi(p^e) = p^{e-1}(p-1),$$

so indeed $\phi(a) \mid \phi(b)$.

For the general case, we factor b:

$$b = p_1^{e_1} \dots p_r^{e_r}, \qquad e_1, \dots, e_r \in \mathbf{Z}_{\geqslant 1}.$$

Since $a \mid b$, we can write

$$a = p_1^{f_1} \dots p_r^{f_r}, \qquad 0 \leqslant f_j \leqslant e_j \text{ for all } j.$$

Then

$$\phi(a) = \phi(p_1^{f_1}) \dots \phi(p_r^{f_r})$$

and

$$\phi(b) = \phi(p_1^{e_1}) \dots \phi(p_r^{e_r}).$$

The fact that $\phi(a) \mid \phi(b)$ then follows from the special case we saw above. □

3.4. Prove that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number.

[**Hint**: Show that for any a, we have $a^{561} \equiv a$ modulo 3, 11, and 17.]

Solution. Let a be an integer. We want to prove that $a^{561} \equiv a \pmod{561}$.

For a prime p, Fermat's little Theorem tells us that $a^p \equiv a \pmod{p}$, therefore given any integers q and r we have $a^{pq+r} \equiv a^{q+r} \pmod{p}$. We can use this to compute a^{561} modulo 3, 11, and 17:

$$\begin{aligned} a^{561} &\equiv a^{187} \equiv a^{62+1} \equiv a^{21} \equiv a^7 \equiv a^{2+1} \equiv a \pmod{3} \\ a^{561} &\equiv a^{51} \equiv a^{4+7} \equiv a \pmod{11} \\ a^{561} &\equiv a^{33} \equiv a^{1+16} \equiv a \pmod{17}. \end{aligned}$$

So a^{561} and a are both solutions of the system of three congruences; by the Chinese Remainder Theorem we have $a^{561} \equiv a \pmod{561}$. □

3.5. Recall that we define $\mathsf{Li} : [2, \infty) \longrightarrow \mathbf{R}$ by

$$\mathsf{Li}\,(x) = \int_2^x \frac{dt}{\log(t)}.$$

(a) Use integration by parts to prove that

$$\mathsf{Li}\,(x) = \frac{x}{\log(x)} + \int_2^x \frac{dt}{(\log(t))^2} + O(1).$$

(b) Fix $x \geqslant 4$ and estimate the two integrals

$$\int_2^{\sqrt{x}} \frac{dt}{(\log(t))^2} \qquad \text{and} \qquad \int_{\sqrt{x}}^x \frac{dt}{(\log(t))^2}.$$

(c) Use part (b) to conclude that $\mathsf{Li}\,(x) \sim x/\log(x)$.

(d) Why was the splitting of the integral into two pieces necessary in part (b)?

Solution.

(a) Write $u = \dfrac{1}{\log(t)}$, $dv = dt$, so $v = t$ and $du = -\dfrac{1}{t(\log(t))^2}$. Integration by parts gives

$$\mathsf{Li}\,(x) = \left[\frac{t}{\log(t)}\right]_2^x + \int_2^x \frac{dt}{(\log(t))^2} = \frac{x}{\log(x)} + \int_2^x \frac{dt}{(\log(t))^2} - \frac{2}{\log(2)}.$$

(b) Since the integrand is a decreasing function, it has a maximum at the start of the interval of integration, so that

$$0 \leqslant \int_2^{\sqrt{x}} \frac{dt}{(\log(t))^2} \leqslant \frac{\sqrt{x} - 2}{(\log(2))^2}$$

and

$$0 \leqslant \int_{\sqrt{x}}^x \frac{dt}{(\log(t))^2} \leqslant \frac{x - \sqrt{x}}{(\log(\sqrt{x}))^2} = \frac{4(x - \sqrt{x})}{(\log(x))^2}.$$

(c) We have

$$\lim_{x\to\infty} \frac{(\sqrt{x}-2)/(\log(2))^2}{x/\log(x)} = \lim_{x\to\infty} \frac{(\log(x))\sqrt{x}}{x} = \lim_{x\to\infty} \frac{\log(x)}{\sqrt{x}} = 0$$

and

$$\lim_{x\to\infty} \frac{4(x-\sqrt{x})/(\log(x))^2}{x/\log(x)} = 4 \lim_{x\to\infty} \frac{x-\sqrt{x}}{(\log(x))x} = 0.$$

Therefore, using part (a):

$$\frac{\mathsf{Li}\,(x)}{x/\log(x)} = 1 + \frac{\int_2^x \frac{dt}{(\log(t))^2}}{x/\log(x)} + \frac{O(1)}{x/\log(x)},$$

we get an expression where, as $x \longrightarrow \infty$, the last two summands on the RHS converge to 0.

(d) The same argument applied to the whole integral gives

$$0 \leqslant \int_2^x \frac{dt}{(\log(t))^2} \leqslant \frac{x-2}{(\log(2))^2},$$

but unfortunately

$$\frac{(x-2)/(\log(2))^2}{x/\log(x)}$$

does not converge to 0 as $x \longrightarrow \infty$. □

3.6. From volume 3 of *Sun Tzu Suan Ching*: "We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?"

Solution. We have to solve the system of congruences

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7. \end{aligned}$$

Since $\mathsf{gcd}\,(3,5) = 1$, we can find $u, v \in \mathbf{Z}$ such that $3u+5v = 1$. For example $u = -3$, $v = 2$. Let $x = 3\cdot 3\cdot(-3)+2\cdot 2\cdot 5 = -7$, then x satisfies the first two congruences, and any common solution to the first two congruences is $\equiv -7 \pmod{15}$.

We have therefore reduced the problem to solving

$$\begin{aligned} x &\equiv -7 \pmod{15} \\ x &\equiv 2 \pmod 7. \end{aligned}$$

We proceed in the same manner. We have $1\cdot 15 - 2\cdot 7 = 1$, so we let $x = 2\cdot 1\cdot 15 + 7\cdot 2\cdot 7 = 128 \equiv 23 \pmod{105}$.

So there are 23 things. □

3.7. Show that if 35 is used as the modulus for an RSA scheme, then the encryption exponent must be the same as decryption exponent.

Solution. Note that $35 = 5 \times 7$ and so $\phi(35) = \phi(5 \times 7) = \phi(5) \times \phi(7) = 4 \times 6 = 24$; therefore we must show that if a is coprime to 24 then it is its own modulo 24 inverse or, in other words, that $a^2 \equiv 1 \mod 24$. The integers $0 \leqslant a < 24$ coprime to 24 are $1, 5, 7, 11, 13, 17, 19,$ and 23; furthermore note that $13 \equiv -11 \mod 24$, $17 \equiv -7 \mod 24$, $19 \equiv -5 \mod 24$ and $23 \equiv -1 \mod 24$, so it suffices to show that the squares of the first four integers in that list are congruent to 1 modulo 24:

$$1^2 \equiv 1 \mod 24 \qquad 5^2 = 25 = 24 \times 1 + 1 \equiv 1 \mod 24$$
$$7^2 = 49 = 24 \times 2 + 1 \equiv 1 \mod 24 \qquad 11^2 = 121 = 24 \times 5 + 1 \equiv 1 \mod 24. \qquad \square$$

3.8. In the lectures, we recalled the fact that if K is a field and f is a polynomial of degree n, then f has at most n roots in K.

In particular, this says that if f is a polynomial with integer coefficients such that the leading coefficient is not divisible by p, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n solutions in $\mathbf{Z}/p\mathbf{Z}$.

(a) Give an example of a pair (p, f) showing that this can fail if p is not prime.

(b) Can you find such an example whenever p is not prime?

Solution.

(a) In $\mathbf{Z}/8\mathbf{Z}$, the congruence $4x \equiv 0 \pmod{8}$ has 4 solutions: $0, 2, 4, 6$.

(b) Yes. Suppose p is not prime and write $p = ab$ with $a, b > 1$. Consider the polynomial $f(x) = ax$. The congruence $ax \equiv 0 \pmod{p}$ has at least two solutions: 0 and b. $\square$