Number Theory Solutions

1. (a) Let p be an odd prime and $a, b \in \mathbb{Z}$.

(i) [5 marks] Prove that $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Solution. We have

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots \binom{p}{p-1}ab^{p-1} + b^p,$$

and the statement amounts to showing that $p \mid \binom{p}{i}$ for $1 \leqslant i \leqslant p-1$. There are a few ways to do this. One way is to use the fact that

$$\binom{p}{i} = \frac{p!}{i!(p-i)!},$$

which gives

$$p! = \binom{p}{i} i!(p-i)!.$$

Now the left-hand side has a factor of p, so p must divide one of the factors on the right-hand side. However, $1 \leqslant i < p$, so all of the integers $1, 2, \ldots, i$ are not divisible by p, and thus $i!$ is not divisible by p. Likewise, $p - i < p$, so $(p-i)!$ is not divisible by p. Thus $\binom{p}{i}$ must be divisible by p. We conclude that

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots \binom{p}{p-1}ab^{p-1} + b^p \equiv a^p + b^p \pmod{p}.$$

[S] 5 marks distributed as follows:
- 1 mark for the binomial expansion of $(a+b)^p$
- 4 marks for proving that $p \mid \binom{p}{i}$ for $1 \leqslant i \leqslant p-1$

(ii) [5 marks] Let $\left(\frac{a}{p}\right)$ denote the Legendre symbol. State Euler's criterion and use it to prove $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Solution. Euler's criterion says that if p is an odd prime and $a \in \mathbb{Z}$, then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

To prove the claim, note that Euler's criterion gives

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Finally, $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$ implies $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ since either side is $+1, -1$, or 0, and p is odd.

[B] This is standard material from the lecture notes:
- 2 marks for stating Euler's criterion
- 3 marks for the proof of the identity

(iii) [3 marks] State the law of Quadratic Reciprocity for p, q distinct odd primes.

Solution. If p, q are distinct odd primes, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} = \begin{cases} +\left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}.$$

Full marks will be given for stating one of the equalities involving $\left(\frac{p}{q}\right)$; they need not state both.

[B] This is standard material from the lecture notes:

- If they wrote the statement in terms of conditions on $p, q \pmod 4$, then:
  - 2 marks for conditions on p, q such that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ (that is, $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$)
  - 1 mark for condition on p, q such that $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ (that is, $p \equiv q \equiv 3 \pmod 4$)
- If they didn't write the statement in terms of conditions on $p, q \pmod 4$, then:
  - 1 mark for a relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$
  - 2 additional marks for relating $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ in terms of an exponent of (-1).

(b) [6 marks] Use Pollard's $p-1$ method to find a factor of 1003.

Solution. Let $N = 1003$. The idea is to iteratively compute $a_k \equiv 2^{k!} \pmod N$ and $g_k = \text{hcf}(a_k - 1, N)$, for $k = 1, 2, \ldots$, stopping when g_k is between 1 and N. The trick is to compute $a_1 = 2$, and then for $k \geqslant 2$ use $a_k \equiv a_{k-1}^k \mod N$. We record the values produced by Pollard's $p-1$ method in the table below:

k	$a_k \pmod N$	$\text{hcf}(a_k - 1, N)$
1	2	1
2	$2^2 = 4$	1
3	$4^3 = 64$	1
4	$64^4 \equiv 35$	17

So we find 17 is a factor of 1003, and $1003 = 17 \cdot 59$.

[S] 6 marks distributed as follows:

- 2 marks for describing the method: the definition of a_k and the halting step (the computation of $g_k = \text{hcf}(a_k - 1, N)$ and stopping when g_k is between 1 and N)
- 4 marks for showing work for $k = 1, 2, 3, 4$ and concluding that 17 is a factor of 1003. NB: If a factorization of 1003 is produced merely by trial division, no marks are to be given.

(c) [6 marks] Solve $102^{70} - 1 \equiv x^{37} \pmod{113}$.

Solution. Note that

$$\begin{aligned} 102^{70} \equiv (-11)^{70} &\equiv (11^2)^{35} \pmod{113} \\ &\equiv 8^{35} \pmod{113} \\ &\equiv 2^{105} \pmod{113}. \end{aligned}$$

Since $2^{14} \equiv -1 \pmod{113}$, we have $2^{28} \equiv 1 \pmod{113}$, and we use this to conclude

$$\begin{aligned} 102^{70} &\equiv 2^{105} \pmod{113} \\ &\equiv 2^{28\cdot 3} \cdot 2^{14} \cdot 2^{7} \pmod{113} \\ &\equiv (1)(-1)(128) \pmod{113} \\ &\equiv 98 \pmod{113}. \end{aligned}$$

This gives $102^{70} - 1 \equiv 97 \pmod{113}$. Now we would like to solve

$$11^{70} - 1 \equiv 97 \equiv x^{37} \pmod{113}.$$

The key is to find an exponent d such that $37d = 1 \pmod{\phi(113)}$, or in other words, to find the multiplicative inverse of 37 in $(\mathbb{Z}/113\mathbb{Z})^{\times}$, which we do using Lemma 1.9 in the lecture notes (carrying out the Extended Euclidean Algorithm). We find that

$$112 + 37 \cdot (-3) = 1,$$

or that $d = -3 \equiv 109 \pmod{112}$. Taking

$$x^{37} \equiv 97 \pmod{113},$$

and exponentiating by d gives

$$\begin{aligned} x^{37(-3)} \equiv x^{1} &\equiv 97^{-3} \pmod{113} \\ &\equiv (-16)^{109} \pmod{113} \\ &\equiv -1 \cdot 2^{436} \pmod{113} \\ &\equiv -1 \cdot 2^{15\cdot 28+16} \pmod{113} \\ &\equiv -1 \cdot 2^{16} \pmod{113} \\ &\equiv (-1)(-4) \pmod{113} \\ &\equiv 4 \pmod{113}. \end{aligned}$$

We conclude that $x = 4 \pmod{113}$.

[N] 6 marks distributed as follows:

- 2 marks for computing $102^{70} \pmod{113}$
- 2 marks for computing the multiplicative inverse of $37 \pmod{112}$
- 2 marks for the solution x