ITCS 531: Number Theory 3 solutions

Rob Egrot

Q1

Prove that if $a, b, c \in \mathbb{Z}$, with $a|bc$, and a and b be coprime, then $a|c$.

- Can't use lemma 1.11 directly as a is not prime.
- Since a, b coprime take x, y with $ax + by = 1$ (Bézout).
- So $axc + byc = c$.
- As $a \mid bc$ we have $bc = ak$ for some k.
- So $axc + ayk = c$.
- So $c = a(xc + yk)$. I.e. $a \mid c$.

Q2

Find all solutions to $x^2 - 1 \equiv_8 0$. What does this tell us about Lagrange's theorem in the case where p is not prime?

- The solutions are $1, 3, 5, 7$.
- This tells us that Lagrange's theorem is false when p is not prime.

Q3

Calculate $5^{30,000} - 6^{123,456} \mod 31$.

- We have $5^{30000} = 5^{30(1000)}$, and $5^{30} \equiv_{31} 1$ by Fermat's little theorem.
- So $5^{30000} \equiv_{31} 1^{1000} \equiv_{31} 1$.
- Also, $123456 = 30(4115) + 6$, so

$$\begin{aligned}
6^{123456} &= 6^{30(4115)+6} \\
&= 6^{30(4115)}.6^6 \\
&\equiv_{31} 1^{4115}.6^6 \text{ using Fermat's little theorem} \\
&\equiv_{31} 6^2.6^2.6^2 \\
&\equiv_{31} 5.5.5 \\
&\equiv_{31} 125 \\
&\equiv_{31} 1.
\end{aligned}$$

So $5^{30,000} - 6^{123,456} = 0 \mod 31$.

Q4

a) Prove that when $n = 2$ we have $(n-1)! \equiv_n -1$.

- $(2-1)! = 1 = -1 \mod 2$.

b) Let p be an odd prime. Define
$g(x) = (x-1)(x-2)\dots(x-(p-1))$.

i) What are the roots of g modulo p?

- The roots are $1, 2, \dots, p-1$.

ii) What is the degree of g?

- $p-1$.

iii) What is the leading term of g?

- x^{p-1}.

Q4

c) Define $h(x) = x^{p-1} - 1$. What are the roots of h modulo p?

- p is prime so little theorem says that $a^{p-1} \equiv_p 1$ whenever a and p are coprime.
- In particular, $a^{p-1} \equiv_p 1$ for all $a \in \{1, \ldots, p-1\}$.
- So $h(x) = x^{p-1} - 1$ has roots $1, 2, \ldots, p-1$ mod p (these are all the roots as the degree of h is $p-1$).

Q4

d) Define $f(x) = g(x) - h(x)$. Prove that f_p must be the constant function $f(x) \equiv_p 0$ for all x.

- Leading term of both h and g is x^{p-1}.
- So degree of $g - h$ is at most $p - 2$.
- But every number that is a root of both g and h is also a root of $g - h$.
- So $1, 2, \ldots, p - 1$ are all roots of $g - h$.
- So $g - h$ has at least $p - 1$ roots.
- Since p is prime, Lagrange's theorem says $g - h$ can have at most $p - 2$ roots mod p, otherwise it is zero (mod p).
- As $g - h$ has more than $p - 2$ roots it must be zero (mod p).
- I.e. $g(x) - h(x) \equiv_p 0$ for all x.

Q4

e) Prove that n is prime if and only if $(n-1)! \equiv_n -1$.

- We have proved that if $n = 2$ then $(n-1)! \equiv_n -1$ is true.
- Let n be an odd prime.
- Then $g(x) \equiv_n h(x)$ for all x - i.e. $(x-1)\dots(x-(n-1)) \equiv_n x^{n-1} - 1$.
- With $x = n$ this gives $(n-1)! \equiv_n n^{n-1} - 1 \equiv_n -1$.
- Conversely, suppose $(n-1)! \equiv_n -1$ and choose $1 \leq q < n$ with $q|n$.
- Then as $kn = (n-1)! + 1$ for some k, and as $q|(n-1)!$, we get $q|1$.
- So $q = 1$, and so n must be prime.