Elementary Number Theory - Exercise 5b

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. If p is an odd prime, show that $x^2 \equiv 1 \pmod p$ has exactly 2 incongruent solutions modulo p.

Solution 1. The two obvious solutions are 1 and -1, and these are incongruenct since $1-(-1) = 2$ is not divisible by an odd prime. Moreover, the polynomial $x^2 - 1$ has degree 2 and its coefficients are not all divisible by p, so Lagrange's Theorem tells us that it has at most two roots modulo p.

Problem 2. Modulo 101, how many roots are there to the polynomial equation

$$x^{99} + x^{98} + \cdots + x + 1 \equiv 0 \pmod{101}?$$

Hint: Multiply with $x(x-1)$.

Solution 2. Let $f(x) = x^{99} + x^{98} + \cdots + x + 1$. Multiplying with $x(x-1)$ we find that

$$f(x)x(x-1) = (x^{101} + x^{100} + \cdots + x^2) - (x^{100} + x^{99} + \cdots + x^2 + x) = x^{101} - x.$$

By Fermat's Little Theorem, $x^{101} \equiv x \pmod{101}$, so we obtain

$$f(x)x(x-1) \equiv 0 \pmod{101}$$

for every x. This implies that, apart from $x = 0$ and $x = 1$ (which are not roots of $f(x)$), every other $x \in \mathbb{Z}/101\mathbb{Z}$ must be a root of $f(x)$. These are 99 roots (Note that Lagrange's Theorem tells us that there cannot be more than 99 roots, but in this case it is clear that $x = 0$ and $x = 1$ are not roots).

Problem 3. Show that, if $n > 4$ is composite, then n divides $(n-1)!$.

Solution 3. Let $n = ab$ with $1 < a, b < n$ be compositite, and $n > 4$. Then $a + b \leq ab - 1 = n - 1$, so we can write

$$(n-1)! = 1 \cdot 2 \cdots a \cdot (a+1) \cdots (a+b) \cdots (ab-1).$$

Since a appears in the product, it divides $(n-1)!$. So it suffices to show that b divides the product $(a+1) \cdots (a+b)$. Indeed, any sequence of b consecutive integers contains a number divisible by b, so some number between $(a+1), \ldots, (a+b)$ is a multiple of b. Hence $n = ab$ divides $(n-1)!$.

Problem 4. Let p be a prime. Wilson's Theorem tells us that $(p-1)! + 1 = kp$ for some $k \in \mathbb{N}$. When is $k = 1$ or $k = p$?

Solution 4. The idea is that $(p-1)!$ grows much faster than p or p^2 (in fact, exponentially fast), so there can only be finitely many primes p with $k = 1$ or $k = p$. For $k = 1$ and $p > 3$ we estimate

$$(p-1)! + 1 = 1 \cdot 2 \cdot \dots \cdot (p-1) + 1 > (p-1) + 1 = p,$$

where used that the factors 2 and $(p-1)$ both appear in the product. Hence $k = 1$ is only possible for $p \leq 3$. Indeed, we have $(2-1)! + 1 = 2$ and $(3-1)! + 1 = 3$ which are the only two possibilities for $k = 1$.

Similarly, for $p > 5$ we have

$$(p-1)! + 1 = 1 \cdot 2 \cdot 3 \cdots \frac{p+1}{2} \cdots (p-1) + 1 > 2 \cdot \frac{p+1}{2} \cdot (p-1) + 1 = p^2$$

where we used that $2, 3, \frac{p+1}{2}$, and $(p-1)$ are different factors in the product if $p > 5$. For $p = 5$ we have $(5-1)! + 1 = 25$, so this is the only possibility for $k = p$.

Problem 5. Find the remainder when 98! is divided by 101.

Solution 5. Since 101 is prime, by Wilson's Theorem we have $100! \equiv -1 \pmod{101}$, which can be written as

$$98! \cdot 99 \cdot 100 \equiv -1 \pmod{101}.$$

Hence we need to invert 99 and 100 modulo 101. This becomes much easier if we use their representatives -2 and -1, instead. The inverse of -1 is -1, and the inverse of -2 is 50 (one can guess this if we recall that we are looking for b, k such that $-2b + 101k = 1$, or one can compute it as $(-2)^{\varphi(101)-1} = (-2)^{99}$ using repeated squaring). Hence we have

$$98! \equiv (-1) \cdot (-2)^{-1} \cdot (-1)^{-1} \equiv (-1) \cdot 50 \cdot (-1) \equiv 50 \pmod{101},$$

so the remainder of 98! divided by 101 is 50.

Problem 6. Compute $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ for $p = 7$ and $p = 11$ to convince yourself that Wolstenholme's Theorem works.

Solution 6. We have $1 + \frac{1}{2} + \cdots + \frac{1}{6} = \frac{49}{20}$, whose denominator is divisible by 7^2, and $1 + \frac{1}{2} + \ldots \frac{1}{10} = \frac{7381}{2520}$, where $7381 = 11^2 \cdot 61$ is divisible by 11^2.

Problem 7. Let $p > 3$ be a prime. Show that

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

Hint: Relate the binomal coefficient to a special value of $h(x) = (x-1)(x-2)\cdots(x-(p-1))$ and use the first claim in Wolstenholme's Theorem.

Solution 7. Again, we consider the polynomial

$$h(x) = (x-1)(x-2)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_2x^2 + a_1x + (p-1)!$$

where the coefficients $a_1, \ldots, a_{p-2}$ are all divisible by p as shown in the proof of Wilson's Theorem. We write

$$\begin{aligned}\binom{2p-1}{p-1} &= \frac{(2p-1)!}{(p-1)!p!} \\ &= \frac{(2p-1)(2p-2)\cdots(2p-(p-1))}{(p-1)!} \\ &= \frac{h(2p)}{(p-1)!} \\ &= 1 + \frac{(2p)^{p-1} + \sum_{j=1}^{p-2} a_j (2p)^j}{(p-1)!}\end{aligned}$$

Since all coefficients a_j are divisible by p, and a_1 is divisible by p^2 by Wolstenholme's Theorem from the lecture, and $(p-1)!$ is coprime to p, we see that the quotient vanishes modulo p^3. This gives the stated result.

Problem 8 (sage)**.** Check the following conjecture numerically: If $p > 3$ is prime, and we write $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b}$ with $\gcd(a, b) = 1$, then $\frac{a}{p^2}$ is square-free.