MATH 152: MIDTERM SOLUTIONS

K. Soundararajan

NOTE: Proofs/explanations are needed for all problems. All the best!

1. Consider the group of reduced residue classes $\pmod{1001}$. (Note $1001 = 7 \times 11 \times 13$). What is the largest possible order of an element of this group? You must also prove that there are elements of this order.

Solution. Let a be a reduced residue class $\pmod{1001}$. Since $a^6 \equiv 1 \pmod 7$, $a^{10} \equiv 1 \pmod{11}$ and $a^{12} \equiv 1 \pmod{13}$ we have that $a^{60} \equiv 1 \pmod{1001}$; note 60 is the l.c.m. of 6, 10 and 12.

On the other hand, pick a primitive root $g_1 \pmod 7$, a primitive root $g_2 \pmod{11}$ and a primitive root $g_3 \pmod{13}$. If we choose $g \equiv g_1 \pmod 7$, $\equiv g_2 \pmod{11}$, and $g_3 \pmod{13}$ then the order of $g \pmod{1001}$ must be a multiple of 6, 10 and 12, and thus a multiple of 60. So the order of $g \pmod{1001}$ is 60 as needed.

2. Let $\ell \geq 2$ be a natural number and let p be a prime with $p \equiv 1 \pmod{\ell}$. Consider the congruence $x^\ell \equiv a \pmod p$ for $(a,p) = 1$. Prove that there are $(p-1)/\ell$ reduced residue classes a for which this congruence has ℓ solutions, and for the remaining reduced residue classes the congruence has no solutions.

Solution. Let g be a primitive root $\pmod p$. If $a \equiv g^{\ell k} \pmod p$ for some integer $0 \leq k < (p-1)/\ell$ then the congruence $x^\ell \equiv a \pmod p$ has the ℓ solutions $x \equiv g^{k+j(p-1)/\ell}$ for $0 \leq j < \ell$. Since the congruence has at most ℓ solutions, it follows that for such a there are exactly ℓ solutions. Note that there are $(p-1)/\ell$ such values of a.

On the other hand, if $x^\ell \equiv a \pmod p$ for some x, then writing $x = g^k$ we find that $a \equiv g^{k\ell} \pmod p$. Thus there are $(p-1)/\ell$ values of a for which the congruence has ℓ solutions, and for the remaining values of a there are no solutions.

3. Is it true that there is a rational number x with $|x|_2 \geq 1024$, $|x-1|_3 \leq 1/27$ and $|x-2|_5 = 25$? Here $|x|_p$ denotes the p-adic absolute value of x. You must explain your answer.

Solution. Yes. Write $x = a/b$ for natural numbers a and b with $(a,b) = 1$. The condition $|x|_2 \geq 1024$ is met by requiring $1024|b$. The condition $|x-2|_5 = 25$ is met by requiring $25\|b$. Thus choose $b = 1024 \times 25 = 25600$. The remaining condition is that $|x-1|_3 \leq 1/27$ which means $27|(a-25600)$. Choose $a = 25627$ and we are done.

4. (a). Let n be an odd natural number with $n \equiv 5 \pmod{13}$. Prove that the congruence $x^2 \equiv 13 \pmod{n}$ has no solutions.

(b). Suppose n is odd and $n \equiv 1 \pmod{13}$. Is it necessarily true that the congruence $x^2 \equiv 13 \pmod{n}$ has a solution?

Solution. Note that the problem did not specify n to be prime.

(a). Note that $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = -1$. So since n is a quadratic non-residue (mod 1)3, we know that n must be divisible by some prime p which is a quadratic non-residue $\pmod{13}$. But if $x^2 \equiv 13 \pmod{n}$ has a solution, then so does $x^2 \equiv 13 \pmod{p}$. That is, $\left(\frac{13}{p}\right) = 1$. But this contradicts quadratic reciprocity: $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = -1$. So the congruence $x^2 \equiv 13 \pmod{n}$ does not have a solution.

(b). This is not necessarily true, since n could be the product of two primes (say) which are both quadratic non-residues (mod 1)3. For example take $n = 5 \times 47$. If $x^2 \equiv 13 \pmod{n}$ then we'd have $x^2 \equiv 13 \pmod{5}$ which is impossible.