MATH 124 HOMEWORK #3

INNA ZAKHAREVICH

(mod (* 7 31) 72)

(1) (a) First, notice that $10^2 \equiv 27 \pmod{73}$. Then $27^2 \equiv (20+7)^2 \equiv 4 \cdot 27 + 4 \cdot (-3) + 49 \equiv 4 \cdot 24 + 49 \equiv 23 + 49 \equiv -1$. Thus $10^8 \equiv 1 \pmod{73}$.
We know that $2^6 = 64 \equiv -9 \pmod{73}$. Then $2^9 = 2^6 \cdot 2^3 \equiv -72 \equiv 1 \pmod{73}$, as desired.

(b) Notice that the order of 2 is 9. We know that $72 | (\operatorname{ord} 2)(\operatorname{ind}_g 2) = 9(\operatorname{ind}_g 2)$ for all g. Thus we see that $8 | \operatorname{ind}_g 2$.
Similarly, we know that $p | \operatorname{ind}_g 10$. In addition, we know that the index of 10 must be odd, since its order is 8. Thus the index of 10 can be $9, 27, 45$ or 63.

(c) Suppose that g is a primitive root. We know that $\operatorname{ind}_g 10 = 9k$ for an odd k, and that $\operatorname{ind}_g 2 = 8\ell$; notice that ℓ is not divisible by 3 because the order of 2 is 9. Thus $\operatorname{ind}_g 20 = 9k + 8\ell$. But notice that $9k + 8\ell$ will be odd, since k is odd; since 8ℓ is not divisible by 3, this is not divisible by 3. Thus we see that $(9k + 8\ell, 72) = 1$, so $20 = g^c$ with $(c, 72) = 1$ and therefore 20 is a primitive root.

(d) By taking each of the exponents mod 72, we can reduce the equations to the following form:

$$\begin{aligned} x^{32} &\equiv 2 \\ x^{63} &\equiv 10 \\ x^{61} &\equiv 47 \\ x^{32} &\equiv 57 \end{aligned}$$

Since $2 \equiv 5^8$, we know that the first equation is equivalent to asking when $x^4 \equiv 5$. Notice that since 5 is a primitive root, there is no primitive root that can be taken to a power divisible by 4 to produce 5 (since, after all, primitive roots are obtained by powers which are relatively prime to 72). Thus the first equation has no solution.
We know that $10 = 5^9$. Thus the second equation is equivalent to asking if there exists an x such that $x^7 \equiv 5$. Let $a = 7{-}1 \pmod{72}$. Then $(5^a)^7 \equiv 5^{7a} \equiv 5 \pmod{73}$, so the second equation has a solution.
Notice that 61 is invertible modulo 72. Let $a \equiv 61^{-1} \pmod{72}$. Then $x \equiv x^{61a} \equiv 47^a \pmod{7}2$, so such an x exists.
Notice that $57^{-1} \equiv 32 \equiv 5^{40} \equiv 5^{-32} \pmod{73}$. Thus we know that $5^{32} \equiv 57 \pmod{73}$, so the last equation also has a solution.

(2) (a) First, write $k = (k, p-1)m$. We claim that $x^k \equiv a$ has a solution if and only if $x^{(k,p-1)} \equiv a$ has a solution. Indeed, suppose that $x^k \equiv a$. But $bk = bm(k, p-1)$ so $(x^m)^{(k,p-1)} \equiv a \pmod{p}$, so we have a solution to $x^{(k,p-1)} \equiv a$. Now suppose that we have a solution to $x^{(k,p-1)} equiva$. For some primitive root g, $x = g^b$ and $a = g^c$, and we have $bk \equiv c \pmod{p-1}$. But we know that

m is invertible mod $p-1$ (by definition), so we have $x = (g^{m^{-1}})^{bm}$. But $a = x^{(k,p-1)} = ((g^{m^{-1}})^{bm})^{(k,p-1)} = (g^{m^{-1}})^{bm(k,p-1)} = (g^{m^{-1}})^k$, so we have a solution to $x^k \equiv a \pmod{p}$. So we have proven the above claim.

What remains to show is that if $k|p-1$, then $x^k \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/k} \equiv 1 \pmod{p}$. First, suppose that $x^k \equiv a \pmod{p}$. Then we know that $1 \equiv (x^k)^{(p-1)/k} \equiv a^{(p-1)/k}$, so we are done. Now suppose that we have $a^{(p-1)/k} \equiv 1 \pmod{p}$. Then we know that $\operatorname{ord} a | (p-1)/k$. But since $p-1|(\operatorname{ord} a)(\operatorname{ind}_g a)$ for all g, we know that $p-1|(\operatorname{ind}_g a)((p-1)/k)$. In particular, we know that for some m, $(p-1)m = (\operatorname{ind}_g a)\frac{p-1}{k}$. Dividing both sides by $p-1/k$, we get $km = \operatorname{ind}_g a$ for some integer m. Then setting $x = g^m$ we have a solution to $x^k \equiv a \pmod{p-1}$.

(b) If the condition given in (a) does not hold then we have zero solutions to the equation (1). Now suppose that we have two solutions $x^k \equiv a$ and $y^k \equiv a$. Then we know that $(x/y)^k \equiv 1$, so x/y is a k-th root of unity. Also, clearly, if α is a k-th root of unity then if $x^k \equiv a$ holds, then $(x\alpha)^k \equiv a$ will also hold. Thus we see that if there is a solution there is a solution for each k-th root of unity. Thus all we need to do is count roots of unity.

Let g be a primitive root. We know that g^c is a k-th root of unity if and only if $p-1|ck$. Thus we need to count c such that $p-1|ck$, for $0 \leq c \leq p-2$. $p-1|ck$ if and only if $p-1/(k,p-1)|c(k/(p-1,k))$, Howver, $(p-1/(k,p-1))$ and $k/(k,p-1)$ are relatively prime, so this happens if and only if $p-1/(k,p-1)|c$. Clearly, there are exactly $(k,p-1)$ such numbers between 0 and $p-2$, so we are done.

Suppose that g is a primitive root, and that a has index α. Then the solutions are $g^{\alpha/k+c}$, where $c = \beta\frac{p-1}{(k,p-1)}$.

(c) Applying the condition in part (a), we need to see whether $6^5 \equiv 1 \pmod{1}01$. $6^5 = 32 \cdot 3^5 \equiv 96 \cdot 3^4 \equiv -5 \cdot 81 \equiv 5 \cdot 20 = -1 \not\equiv 1 \pmod{101}$, so the first equation has no solutions. The second equation has $(-6)^5 = -6^5 \equiv 1 \pmod{101}$, so the second equation has 20 solutions.

Now consider the last equation. First, note that if $p = 1$ then the equation has exactly one solution. Now, suppose that p is odd. We know that this equation has solutions exactly when $(-1)^{p-1/(p-1,8)} \equiv 1 \pmod{p}$. But this means exactly that $p-1/(p-1,8)$ is even. Suppose that $p = 2^k m + 1$, with $k > 0$ and m odd. Then $(p-1,8) = 2^{\min(k,3)}$. But then

$$\frac{p-1}{(p-1,8)} = \frac{2^k m}{2^{\min(k,3)}}.$$

Note that if $k \leq 3$ this is equal to m, which is odd; this means that the equation has no solutions. If $k > 3$ this will be $2^{k-3}m$, which is even, so the solution will have $(p-1,8) = 8$ solutions. Thus we see that this equation has 8 solutions when $p = 16n+1$, and zero solutions for all other p.

(3) (a)

$$\left(\frac{-26}{73}\right) = \left(\frac{-1}{73}\right)\left(\frac{2}{73}\right)\left(\frac{13}{73}\right) = 1 \cdot 1 \left(\frac{73}{13}\right) = \left(\frac{8}{13}\right) = -1.$$

$$\left(\frac{19}{73}\right) = \left(\frac{73}{19}\right) = \left(\frac{-3}{19}\right) = \left(\frac{3}{19}\right) = -\left(\frac{19}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$
$$\left(\frac{33}{73}\right) = \left(\frac{3}{73}\right)\left(\frac{11}{73}\right) = \left(\frac{73}{3}\right)\left(\frac{73}{11}\right) = \left(\frac{1}{3}\right)\left(\frac{-4}{11}\right) = -1.$$

(b) (i)
$$\left(\frac{-7}{1009}\right) =$$

(ii)
$$\left(\frac{5}{229}\right) = \left(\frac{229}{5}\right) = \left(\frac{-1}{5}\right) = 1.$$

(iii)
$$\left(\frac{125}{227}\right) = \left(\frac{5}{227}\right) = \left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

(c) Note that
$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right).$$
So this will be one exactly when $\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right)$. These will both be 1 if $p \equiv \pm 1 \pmod 8$ and $p \equiv pm1 \pmod 5$, meaning that $p \equiv \pm 1, \pm 9, \pmod{40}$. These will both be -1 when $p \equiv \pm 3 \pmod 8$ and $p \equiv \pm 2 \pmod 5$, meaning that $p \equiv \pm \pm 3, \pm 13 \pmod{40}$. Thus $\left(\frac{10}{p}\right) = 1$ exactly when $p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$.

(4) (a) Suppose there were finitely many primes of the form $3n-1$: $p_1, \ldots, p_n$. Consider the number $k = 3(p_1 \cdots p_n) - 1$. This is congruent to -1 mod 3. If all prime factors of it were 1 mod 3, the number itself would be 1 mod 3; however, this is not the case. Thus it has a factor which is -1 mod 3 which is not one of $p_1, \ldots, p_n$; contradiction. Thus there are infinitely many primes of the form $3n - 1$.

(b) (i) Let $a = -3$. Notice that $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. The first of these will be 1 if $p \equiv 1 \pmod 4$. The second of these will be one if $p \equiv \pm 1 \pmod{12}$. Thus they will both be 1 when $p \equiv 1 \pmod{12}$. The first of these will be -1 if $p \equiv 2 \pmod 4$, and the second will be -1 when $p \equiv \pm 5 \pmod{12}$, so both will be -1 when $p \equiv 7 \pmod{12}$. Thus we have $\left(\frac{-3}{p}\right) = 1$ when $p \equiv 1, 7 \pmod{12}$, which happens exactly when $p \equiv 1 \pmod 6$, which happens exactly when $p \equiv 1 \pmod 3$ (since p clearly can't be 4 mod 6).

(ii) Suppose there were only finitely many primes of the form $3n+1$, $p_1, \ldots, p_n$. Consider the number $k = (p_1 \cdots p_n^2 + 3$. This will also be of the form $3n + 1$, and none of the p_i will divide it. Consider a divisor d of k. We know that the equation $x^2 \equiv -3 \pmod d$ has a solution, since we can just use $x = p_1 \cdots p_n$. Thus any prime divisor must be of the form $3m + 1$, and therefore (since none of the p_i divide k) we must have another prime of the form $3m + 1$. Contradiction. Therefore, there are infinitely many primes of the form $3n + 1$.