

SOLUTIONS TO HOMEWORK 5  
Math 104B - Dr. Evans  
UCSD Spring 2004

1. Let  $p > 2$  and let  $x$  be a  $p$ -adic number such that  $x^p = 1$ . We proved that  $x$  must be 1, as follows. If  $x$  is not 1, then  $x$  must have the form  $x = 1 + tp^r$ , where  $t$  is a  $p$ -adic unit and  $r$  is some positive integer. Thus  $1 = x^p = (1 + tp^r)^p$ . By the binomial theorem, the right side has the form  $1 + tp^{r+1} + Mp^{2r+1}$ , for some  $p$ -adic integer  $M$ . Bringing the first two of these terms over to the left, we get (after cancellation)  $-t = Mp^r$ , which contradicts the fact that  $t$  is a  $p$ -adic unit.
- For this problem, show precisely where this proof breaks down in the case  $p = 2$ . (Hint: Look carefully at the binomial theorem.)

Suppose  $x = 1 + tp^r$  where  $p \nmid t$ ,  $r \geq 1$  satisfies  $x^p = 1$ . By the binomial theorem,

$$\begin{aligned} 0 &= x^p - 1 = (1 + tp^r)^p - 1 \\ &= 1 + \binom{p}{1} tp^r + \binom{p}{2} t^2 p^{2r} + \dots - 1 \\ &= \binom{p}{1} tp^r + \binom{p}{2} t^2 p^{2r} + \dots \end{aligned}$$

Now  $\binom{p}{1} = p$  for all  $p$ , and  $\binom{p}{2}$  is also divisible by  $p$  when  $p > 2$ . In the original proof, every term after the first one is divisible by  $p^{2r+1}$ . When  $p = 2$ ,  $\binom{p}{2} = 1$  is not divisible by 2. This is precisely where the proof goes wrong. There is only one term after the first one, and it is only divisible by  $p^{2r}$ :

$$\begin{aligned} 0 &= x^2 - 1 = (1 + t2^r)^2 - 1 \\ &= 1 + 2t2^r + t^2 2^{2r} - 1 \\ &= t2^{r+1} + t^2 2^{2r} \\ &= t2^{r+1}(1 + t2^{r-1}) \end{aligned}$$

Since  $t$  is a  $p$ -adic unit,  $t \neq 0$ , so we must have  $1 + t2^{r-1} = 0$ . Letting  $r = 1$ , we see that  $t = -1$  is a legitimate solution. Hence, no contradiction is reached.

2. Let  $p = 13$ . For every positive integer  $n$ , let  $f(n)$  denote the number of distinct primitive  $p$ -adic  $n^{\text{th}}$  roots of unity. Find  $f(1)$ ,  $f(2)$ , ...,  $f(30)$ . (Hint:  $f(12) = 4$  and  $f(15) = 0$ .)

Recall that  $\mathbb{Q}_p$  contains exactly the  $(p-1)^{\text{th}}$  roots of unity. When  $p = 13$ , there are twelve  $12^{\text{th}}$  roots of unity. Also recall that a primitive  $n^{\text{th}}$  root of unity has exactly order  $n$ . The roots of unity form a cyclic group and are all powers of a primitive  $12^{\text{th}}$  roots of unity  $\zeta$ . Finally, we have

$$\text{ord}(\zeta^k) = \frac{\text{ord } \zeta}{\gcd(\text{ord } \zeta, k)} = \frac{12}{\gcd(k, 12)}$$

In particular, the order of an element divides 12. Hence, there cannot be any elements of order  $n$  if  $n$  does not divide 12. If  $n$  does divide 12, then the number of elements of order  $n$  equal the

number of  $k$  between 1 and 12 such that  $n = \frac{12}{\gcd(k,12)}$ . For this to happen,  $k$  must equal  $\frac{12}{n}$  times something relatively prime to  $n$ . Hence, there are  $\phi(n)$  elements of order precisely  $n$ . Therefore,

$$f(n) = \begin{cases} \phi(n) & \text{if } n \mid 12 \\ 0 & \text{if } n \nmid 12 \end{cases}$$

3. Problem #2 mentioned four primitive  $p$ -adic 12<sup>th</sup> roots of unity, where  $p = 13$ . Give the first  $p$ -adic digit of each of these four roots of unity.

The 12 roots of unity in  $\mathbb{Q}_{13}$  have first digit  $1, 2, \dots, 12$ . The order of a root of unity starting with  $a_0$  has the same order as  $a_0$  has in the integers modulo  $p$  under multiplication:

$$\text{ord}(\zeta) = \text{ord}_p(a_0)$$

$a_0 = 1$  has order 1 in the integers modulo  $p$ , so it gives a primitive 1<sup>st</sup> root of unity.  $a_0 = 2$  has order 12 in the integers modulo  $p$ , since  $2^4 \equiv 3 \pmod{13}$  and  $2^6 \equiv 12 \pmod{13}$ . Hence, the root of unity  $\zeta$  starting with  $a_0 = 2$  is a primitive 12<sup>th</sup> root of unity. To find the other primitive roots of unity, we make use of the fact mentioned in the previous problem:

$$\text{ord}(\zeta^k) = \frac{\text{ord } \zeta}{\gcd(\text{ord } \zeta, k)} = \frac{12}{\gcd(k, 12)}$$

In particular,  $\zeta^k$  has order 12 if and only if  $k$  is relatively prime to 12. There are four such numbers between 1 and 12:  $k = 1, 5, 7, 11$ . The first digits of  $\zeta^1, \zeta^5, \zeta^7$ , and  $\zeta^{11}$  are given by  $a_0^1, a_0^5, a_0^7$ , and  $a_0^{11}$  reduced modulo 13. Therefore, the beginning digits of the four primitive  $p$ -adic 12<sup>th</sup> roots of unity are 2, 6, 11, and 7.

4. Let  $p = 7$ . Show that the two  $p$ -adic zeros of  $f(x) = px^2 + x - 1$  have the following initial  $p$ -adic expansions:

$$\begin{aligned} x_1 &= 1 + 6 \cdot 7 + 1 \cdot 7^2 + \dots \\ x_2 &= 6 \cdot \frac{1}{7} + 5 + 5 \cdot 7^2 + \dots \end{aligned}$$

Guess the counterparts of these expansions when  $p = 109$  in place of  $p = 7$ , using pattern recognition (no work need be shown).

Factor  $f(x)$  as  $px^2 + x - 1 = (x - \alpha)(px - \beta)$ . The roots of the polynomial are  $\alpha$  and  $\frac{\beta}{p}$ . Comparing the coefficient of  $x$  on both sides gives  $1 = -p\alpha - \beta$ , or  $\frac{\beta}{p} = -\frac{1}{p} - \alpha$ . So once we've found  $\alpha$ , we can plug into this equation and solve for  $\beta$ .

We see that  $f(x) \equiv x - 1 \equiv 0 \pmod{p}$  has the solution  $a_0 = 1$ , and  $f'(1) = 2p + 1 \not\equiv 0 \pmod{p}$ . Suppose  $\alpha_2 = 1 + a_1p$ . Assuming  $f(\alpha_2) \equiv 0 \pmod{p^2}$ , we want to solve for  $a_1$ . By Taylor's Theorem,

$$0 \equiv f(\alpha_2) = f(1 + a_1p) \equiv f(1) + f'(1)a_1p \pmod{p^2}$$

Since  $f(1) = p$  and  $f'(1) \equiv 1 \pmod{p}$ , we have

$$\begin{aligned} 0 &\equiv p + a_1p && \pmod{p^2} \\ a_1p &\equiv -p && \pmod{p^2} \\ a_1 &\equiv -1 \equiv p-1 && \pmod{p} \end{aligned}$$

Hence,  $\alpha_2 = 1 + (p-1)p$ .

Now assume  $\alpha_3 = 1 + (p-1)p + a_2p^2 = \alpha_2 + a_2p^2$  and that  $f(\alpha_3) \equiv 0 \pmod{p^3}$ . After some painful algebra,  $f(\alpha_2) = f(p^2 - p + 1) = p^5 - 2p^4 + 3p^3 - p^2 \equiv -p^2 \pmod{p^3}$  and  $f'(\alpha_2) \equiv f'(1) \equiv 1 \pmod{p}$ . By Taylor's Theorem,

$$0 \equiv f(\alpha_3) = f(\alpha_2 + a_2p^2) \equiv f(\alpha_2) + f'(\alpha_2)a_2p^2 \equiv -p^2 + a_2p^2 \pmod{p^3}$$

Hence,  $a_2 = 1$  and  $\alpha_3 = 1 + (p-1)p + p^2$ . We have solved for the first three digits of  $\alpha$ :

$$\alpha = 1 + (p-1)p + p^2 + \dots$$

Plugging in for  $\frac{\beta}{p}$ , we have

$$\begin{aligned} \frac{\beta}{p} &= -p^{-1} - \alpha \\ &= -p^{-1} - (1 + (p-1)p + p^2 + \dots) \\ &= (p-1)p^{-1} - 1 - (1 + (p-1)p + p^2 + \dots) \\ &= (p-1)p^{-1} - 2 - (p-1)p - p^2 - \dots \\ &= (p-1)p^{-1} + (p-2) - p - (p-1)p - p^2 - \dots \\ &= (p-1)p^{-1} + (p-2) - p^2 - p^2 - \dots \\ &= (p-1)p^{-1} + (p-2) - 2p^2 - \dots \\ &= (p-1)p^{-1} + (p-2) + (p-2)p^2 + \dots \end{aligned}$$

When  $p = 7$ , we have

$$\begin{aligned} \alpha &= x_1 = 1 + 6p + p^2 + \dots \\ \frac{\beta}{p} &= x_2 = 6p^{-1} + 5 + 5p^2 + \dots \end{aligned}$$

and when  $p = 109$ , we have

$$\begin{aligned} \alpha &= x_1 = 1 + 108p + p^2 + \dots \\ \frac{\beta}{p} &= x_2 = 108p^{-1} + 107 + 107p^2 + \dots \end{aligned}$$

5. Show that  $x^4 - 17 = 2y^2$  has solutions  $x, y$  in  $\mathbb{Q}_p$  for all  $p$ .

By plugging in certain values for  $x$  or  $y$ , we can sometimes solve for the other variable modulo  $p$ . By creating three conditions such that (almost) every prime has a solution in at least one of these situations, then there exists solutions in  $\mathbb{Q}_p$  for (almost) every prime.

Let  $x = 5$ . Solving for  $y$ , we have  $y^2 \equiv 304 = 16 \cdot 19 \pmod{p}$ . This has a solution  $y = a_0$  modulo  $p$  if  $\left(\frac{19}{p}\right) = 1$ . By Hensel's Lemma, this extends to a solution for  $y$  in  $\mathbb{Z}_p$  with the same beginning digit. Hence,  $x = 5$ ,  $y = a_0 + \dots$  is a solution in  $\mathbb{Q}_p$ .

Let  $y = 4$ . Solving for  $x$ , we have  $x^4 \equiv 49 \pmod{p}$ , or  $x^2 \equiv 7 \pmod{p}$ . This has a solution  $x = b_0$  modulo  $p$  if  $\left(\frac{7}{p}\right) = 1$ . By Hensel's Lemma, this extends to a solution for  $x$  in  $\mathbb{Z}_p$  with the same beginning digit. Hence,  $x = b_0 + \dots$ ,  $y = 4$  is a solution in  $\mathbb{Q}_p$ .

Let  $y = 94$ . Solving for  $x$ , we have  $x^4 \equiv 17689 \pmod{p}$ , or  $x^2 \equiv 133 \pmod{p}$ . This has a solution  $x = c_0$  modulo  $p$  if  $\left(\frac{133}{p}\right) = 1$ . By Hensel's Lemma, this extends to a solution for  $x$  in  $\mathbb{Z}_p$  with the same beginning digit. Hence,  $x = c_0 + \dots$ ,  $y = 94$  is a solution in  $\mathbb{Q}_p$ .

If  $\left(\frac{19}{p}\right) = 1$ , then the first case gives us a solution in  $\mathbb{Q}_p$ . If  $\left(\frac{7}{p}\right) = 1$ , then the second case gives us a solution in  $\mathbb{Q}_p$ . If  $\left(\frac{19}{p}\right) = -1$  and  $\left(\frac{7}{p}\right) = -1$ , then  $\left(\frac{133}{p}\right) = \left(\frac{19}{p}\right)\left(\frac{7}{p}\right) = (-1)(-1) = 1$ , and the third case gives us a solution in  $\mathbb{Q}_p$ .

We must still find a solution when  $p = 2, 7, 19$ , and  $\infty$ , since the Legendre symbol does not apply to these primes. When  $p = 2$ , we must use the strong form of Hensel's Lemma, that  $x^2 = m$  has a solution in  $\mathbb{Z}_2$  iff  $m \equiv 1 \pmod{8}$ . Let  $x = 11$ . Solving for  $y$ , we have  $y^2 = 7312 = 16 \cdot 457$ , or  $\left(\frac{y}{4}\right)^2 = 457$ . Since  $457 \equiv 1 \pmod{8}$ , there is a solution  $\frac{y}{4} = d_0 + d_1 2 + \dots$  in  $\mathbb{Z}_2$ . Hence,  $x = 11$ ,  $y = d_0 2^2 + d_1 2^3 + \dots$  is a solution in  $\mathbb{Q}_2$ .

When  $p = 7$ , let  $x = 3$ . Solving for  $y$ , we have  $y^2 \equiv 32 \pmod{7}$ , which has a solution  $e_0 = 2$  since  $\left(\frac{32}{7}\right) = \left(\frac{4}{7}\right) = 1$ . By Hensel's Lemma, this extends to a solution for  $y$  in  $\mathbb{Z}_7$  with the beginning digit equal to 3. Hence,  $x = 3$ ,  $y = 2 + \dots$  is a solution in  $\mathbb{Q}_7$ .

When  $p = 19$ , let  $x = 1$ . Solving for  $y$ , we have  $y^2 \equiv -8 \pmod{19}$ , which has a solution  $f_0 = 7$  since  $\left(\frac{-8}{19}\right) = \left(\frac{49}{19}\right) = 1$ . By Hensel's Lemma, this extends to a solution for  $y$  in  $\mathbb{Z}_{19}$  with the same beginning digit. Hence,  $x = 1$ ,  $y = 7 + \dots$  is a solution in  $\mathbb{Q}_{19}$ .

Finally,  $p = \infty$  means  $\mathbb{Q}_\infty = \mathbb{R}$ . A solution in the reals is  $y = 0$ ,  $x = \sqrt[4]{17}$ . Hence, we've found a solution in  $\mathbb{Q}_p$  for all  $p \leq \infty$ .