

SOLUTIONS TO HOMEWORK 2
 Math 104B - Dr. Evans
 UCSD Spring 2004

1. Find the 5-adic expansion of -99 .

$$\begin{array}{r} -1 = 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots \\ -98 = 3 + 4 \cdot 5 + 3 \cdot 5^2 + 0 \cdot 5^3 + \dots \\ \hline -99 = 1 + 0 \cdot 5 + 1 \cdot 5^2 + 4 \cdot 5^3 + \dots \end{array}$$

Hence, the 5-adic digits of $-99 = \sum a_n p^n$ are $a_0 = 1$, $a_1 = 0$, $a_2 = 1$, and $a_n = 4$ for all $n \geq 3$.

2. Problem 4 from the book: If $x = a_0 + a_1 p + a_2 p^2 + \dots$, what is $-x$?

Let $-x = b_0 + b_1 p + b_2 p^2 + \dots$. Suppose that $a_0 \neq 0$. Since $x + (-x) = 0$, $a_0 + b_0$ must be a multiple of p . The bounds on a_0 and b_0 imply that $1 \leq a_0 + b_0 \leq 2p - 2$, so the only choice is that $a_0 + b_0 = p$. Hence, $b_0 = p - a_0$. Note that since $1 \leq a_0 \leq p - 1$, we have $1 \leq b_0 \leq p - 1$ as well.

For the second p -adic digits, there will be a p carried over from the first digit, since $a_0 + b_0 = p$. So $a_1 p + b_1 p + p = (a_1 + b_1 + 1)p$ must be a multiple of p^2 . By the bounds on a_1 and b_1 , $1 \leq a_1 + b_1 + 1 \leq 2p - 1$. This forces $a_1 + b_1 + 1 = p$, or $b_1 = (p - 1) - a_1$. Note that since $0 \leq a_1 \leq p - 1$, we have $0 \leq b_1 \leq p - 1$ as well. This process will continue in a similar fashion, so $b_n = (p - 1) - a_n$ for all $n \geq 1$.

If $a_0 = 0$, then we can't define $b_0 = p - a_0 = p$ since it's not in the proper range. So we must define $b_0 = 0$ instead. However, the same process defined above will work if a_0 is replaced by the first nonzero p -adic digit, say a_N for some $N \geq 0$. Such a digit exists, otherwise the p -adic number is 0, which is its own negative.

Here's a little trick that makes this easier. Instead of finding $-x$, we find $-1 - x$. Since

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

there is no borrowing involved when subtracting x . Hence,

$$-1 - x = (p - 1 - a_0) + (p - 1 - a_1)p + (p - 1 - a_2)p^2 + \dots$$

Adding 1 to this p -adic number may involve some carrying until the first nonzero a_N is reached for some $N \geq 0$. Then the p -adic digits of $-x = \sum b_n p^n$ are $b_n = 0$ for $n < N$, $b_N = p - a_N$, and $b_n = (p - 1) - a_n$ for $n > N$.

3. *Problem 18 from the book: Suppose p is an odd prime. Show that if $x^2 \equiv m \pmod{p}$ has a solution and $p \nmid m$, then $x^2 \equiv m \pmod{p^n}$ has a solution for all $n \geq 1$. What happens if $p = 2$?*

Let x_0 be a solution to $x_0^2 \equiv m \pmod{p}$. Note that $m \not\equiv 0 \pmod{p}$ implies $x_0 \not\equiv 0 \pmod{p}$. We will find solution x_n to $x_n^2 \equiv m \pmod{p^{n+1}}$ with

$$\begin{aligned} x_0 &= a_0 \\ x_1 &= a_0 + a_1p \\ x_2 &= a_0 + a_1p + a_2p^2 \\ &\vdots \\ x_{n-1} &= a_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1} \\ x_n &= a_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1} + a_np^n \end{aligned}$$

with $0 \leq a_i \leq p - 1$. With this setup, we may assume $x_n \equiv x_{n-1} \pmod{p^n}$.

The proof is by induction on n . The base case of $n = 1$ is true by assumption. Suppose that x_{n-1} is a solution to $x_{n-1}^2 \equiv m \pmod{p^n}$, that is, $m - x_{n-1}^2 = kp^n$ for some integer k . We want to show this implies a solution to $x_n^2 \equiv m \pmod{p^{n+1}}$. Plugging in the assumption that $x_n = x_{n-1} + a_np^n$ for some integer a_n ,

$$\begin{aligned} x_n^2 &= (x_{n-1} + a_np^n)^2 = x_{n-1}^2 + 2x_{n-1}a_np^n + a_n^2p^{2n} \\ m &\equiv x_n^2 \equiv x_{n-1}^2 + 2x_{n-1}a_np^n \pmod{p^{n+1}} \\ m - x_{n-1}^2 &= kp^n \equiv 2x_{n-1}a_np^n \pmod{p^{n+1}} \\ \frac{m - x_{n-1}^2}{p^n} &= k \equiv 2x_{n-1}a_n \pmod{p} \end{aligned}$$

Note that $x_{n-1} \equiv x_0 \pmod{p}$, so x_{n-1} on the right hand side may be replaced with x_0 . Also note that 2 has an inverse modulo p since p is an odd prime, and x_0 has an inverse modulo p since it is not zero modulo p by assumption. Solving for a_n ,

$$a_n \equiv 2^{-1}x_0^{-1}k \equiv 2^{-1}x_0^{-1}\left(\frac{m - x_{n-1}^2}{p^n}\right) \pmod{p}$$

Since a_n is determined modulo p by the previous x_{n-1} , a_n may be reduced to be in the range $0 \leq a_n \leq p - 1$. Every step in the argument above is reversible, so this shows that $x_n = x_{n-1} + a_np^n$ will be a solution to $x_n^2 \equiv m \pmod{p^{n+1}}$, as desired.

When $p = 2$, there is no way to go from x_{n-1} to x_n . The argument breaks down when one tries to take the inverse of 2 modulo p .

4. Let $p = 7$. The previous problem says that there is a p -adic number

$$x = a_0 + a_1p + a_2p^2 + \dots$$

that satisfies the equation

$$a_0 + a_1p + \dots + a_np^n \equiv 2 \pmod{p^{n+1}}$$

for all n .

(a) Use the technique from the previous problem to explicitly calculate the first three p -adic digits a_0 , a_1 , and a_2 of the solution to the equation $x^2 = 2$. You may assume $a_0 = 4$ (so you really only need to calculate two digits).

Let $x_0 = 4$, and assume $x_1 = 4 + a_1p$. Then

$$\begin{aligned} x_1^2 &= (4 + a_1p)^2 = 16 + 8a_1p + a_1^2p^2 \\ 2 &\equiv 16 + 8a_1p \pmod{p^2} \\ -14 &\equiv 1a_1p \pmod{p^2} \\ 5 &\equiv -2 \equiv a_1 \pmod{p} \end{aligned}$$

Hence, $x_1 = 4 + 5p = 39$. Now assume $x_2 = 39 + a_2p^2$. Then

$$\begin{aligned} x_2^2 &= (39 + a_2p^2)^2 = 1521 + 78a_2p^2 + a_2^2p^4 \\ 2 &\equiv 1521 + 78a_2p^2 \pmod{p^3} \\ -31p^2 &= -1519 \equiv 78a_2p^2 \pmod{p^3} \\ 4 &\equiv -31 \equiv 78a_2 \equiv a_2 \pmod{p} \end{aligned}$$

Therefore, the first three digits of x in \mathbb{Z}_7 are

$$\mathbf{x = 4 + 5p + 4p^2 + \dots}$$

(b) Plugging in $p = 7$ and the digits found in part (a) to get the integers $N = a_0 + a_1p + a_2p^2$. Show by direct calculation that $N^2 - 2$ is divisible by $7^3 = 343$. This shows that N is “close to” the square root of 2 in \mathbb{Z}_7 .

$$\begin{aligned} N &= 4 + 5 \cdot 7 + 4 \cdot 7^2 = 235 \\ N^2 &= 235^2 = 55225 \\ N^2 - 2 &= 55223 = 161 \cdot 343 = 161 \cdot 7^3 \end{aligned}$$

5. Find the first four 2-adic digits for the solutions to $x^2 + x + 2 = 0$ in \mathbb{Z}_2 .

As usual, assume $x = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + \dots$. Both $a_0 = 0$ and $a_0 = 1$ are valid solutions to the equation $x^2 + x + 2 \equiv 0 \pmod{2}$. Hence, there will be two solutions to find.

Case $a_0 = 0$. To solve for a_1 , we plug in $x = 0 + a_1 \cdot 2$ into the equation modulo 4.

$$\begin{aligned}(0 + a_1 \cdot 2)^2 + (0 + a_1 \cdot 2) + 2 &\equiv 0 \pmod{4} \\ 0 + 0 + 2a_1 + 2 &\equiv 0 \pmod{4} \\ 2a_1 &\equiv -2 \equiv 2 \pmod{4} \\ a_1 &\equiv 1 \pmod{2}\end{aligned}$$

To solve for a_2 , we plug in $x = 2 + a_2 \cdot 2^2$ into the equation modulo 8.

$$\begin{aligned}(2 + a_2 \cdot 2^2)^2 + (2 + a_2 \cdot 2^2) + 2 &\equiv 0 \pmod{8} \\ 4 + 2 + 4a_2 + 2 &\equiv 0 \pmod{8} \\ 4a_2 &\equiv -8 \equiv 0 \pmod{8} \\ a_2 &\equiv 0 \pmod{2}\end{aligned}$$

To solve for a_3 , we plug in $x = 2 + a_3 \cdot 2^3$ into the equation modulo 16.

$$\begin{aligned}(2 + a_3 \cdot 2^3)^2 + (2 + a_3 \cdot 2^3) + 2 &\equiv 0 \pmod{16} \\ 4 + 2 + 8a_3 + 2 &\equiv 0 \pmod{16} \\ 8a_3 &\equiv -8 \equiv 8 \pmod{16} \\ a_3 &\equiv 1 \pmod{2}\end{aligned}$$

In this case, the first four 2-adic digits are

$$\mathbf{x = 0 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + \dots}$$

Case $a_0 = 1$. To solve for a_1 , we plug in $x = 1 + a_1 \cdot 2$ into the equation modulo 4.

$$\begin{aligned}(1 + a_1 \cdot 2)^2 + (1 + a_1 \cdot 2) + 2 &\equiv 0 \pmod{4} \\ 1 + 1 + 2a_1 + 2 &\equiv 0 \pmod{4} \\ 2a_1 &\equiv -4 \equiv 0 \pmod{4} \\ a_1 &\equiv 0 \pmod{2}\end{aligned}$$

To solve for a_2 , we plug in $x = 1 + a_2 \cdot 2^2$ into the equation modulo 8.

$$\begin{aligned}(1 + a_2 \cdot 2^2)^2 + (1 + a_2 \cdot 2^2) + 2 &\equiv 0 \pmod{8} \\ 1 + 1 + 4a_2 + 2 &\equiv 0 \pmod{8} \\ 4a_2 &\equiv -4 \equiv 4 \pmod{8} \\ a_2 &\equiv 1 \pmod{2}\end{aligned}$$

To solve for a_3 , we plug in $x = 5 + a_3 \cdot 2^3$ into the equation modulo 16.

$$\begin{aligned}(5 + a_3 \cdot 2^3)^2 + (5 + a_3 \cdot 2^3) + 2 &\equiv 0 \pmod{16} \\ 25 + 5 + 8a_3 + 2 &\equiv 0 \pmod{16} \\ 8a_3 &\equiv -32 \equiv 0 \pmod{16} \\ a_3 &\equiv 0 \pmod{2}\end{aligned}$$

In this case, the first four 2-adic digits are

$$\mathbf{x} = \mathbf{1} + \mathbf{0} \cdot \mathbf{2} + \mathbf{1} \cdot \mathbf{2}^2 + \mathbf{0} \cdot \mathbf{2}^3 + \dots$$

6. Let $p = 5$. Consider the p -adic integers

$$a = 3 + 3p + 3p^2 + 3p^3 + 3p^4 + \dots$$

$$b = 1 + 2p + 3p^2 + 4p^3 + 0p^4 + \dots$$

For the following problems, do not assume that a and b are rational numbers. By direct calculation, do the following:

(a) Find the first five p -adic digits of $a + b$ and $a - b$.

$$\begin{array}{r} a = 3 + 3p + 3p^2 + 3p^3 + 3p^4 + \dots \\ + b = 1 + 2p + 3p^2 + 4p^3 + 0p^4 + \dots \\ \hline a + b = 4 + 5p + 6p^2 + 7p^3 + 3p^4 + \dots \\ = 4 + 0p + 7p^2 + 7p^3 + 3p^4 + \dots \\ = 4 + 0p + 2p^2 + 8p^3 + 3p^4 + \dots \\ = \mathbf{4} + \mathbf{0p} + \mathbf{2p^2} + \mathbf{3p^3} + \mathbf{4p^4} + \dots \\ \\ a = 3 + 3p + 3p^2 + 3p^3 + 3p^4 + \dots \\ - b = 1 + 2p + 3p^2 + 4p^3 + 0p^4 + \dots \\ \hline a - b = 2 + 1p + 0p^2 - 1p^3 + 3p^4 + \dots \\ = \mathbf{2} + \mathbf{1p} + \mathbf{0p^2} + \mathbf{4p^3} + \mathbf{2p^4} + \dots \end{array}$$

(b) Find the first three p -adic digits of $a \cdot b$ and $\frac{a}{b}$.

$$\begin{aligned} a \cdot b &= \left(3 + 3p + 3p^2 + 3p^3 + 3p^4 + \dots\right) \left(1 + 2p + 3p^2 + 4p^3 + 0p^4 + \dots\right) \\ &= (3 \cdot 1) + (3 \cdot 2 + 3 \cdot 1)p + (3 \cdot 3 + 3 \cdot 2 + 3 \cdot 1)p^2 + \dots \\ &= 3 + 9p + 18p^2 + \dots = 3 + 4p + 19p^2 + \dots \\ &= \mathbf{3} + \mathbf{4p} + \mathbf{4p^2} + \dots \end{aligned}$$

Let $\frac{a}{b} = c = \sum c_n p^n$. Then $a = b \cdot c$.

$$\begin{aligned} 3 + 3p + 3p^2 + \dots &= \left(1 + 2p + 3p^2 + \dots\right) \left(c_0 + c_1 p + c_2 p^2 + \dots\right) \\ &= (1 \cdot c_0) + (1 \cdot c_1 + 2 \cdot c_0)p + (1c_2 + 2c_1 + 3c_0)p^2 + \dots \end{aligned}$$

From these equations, $c_0 = 3$, $c_1 = 3 - 2 \cdot c_0 = 3 - 2 \cdot 3 = -3$, and $c_2 = 3 - 2c_1 - 3c_0 = 3 - 2(-3) - 3(3) = 0$. Hence, $c = 3 + (-3)p + 0p^2 + \dots$. However, negative digits are not allowed, so we must borrow $1 \cdot p^2$ to become $5 \cdot p$. Likewise, a p^3 must be borrowed to become $5p^2$. So the final answer is

$$\frac{\mathbf{a}}{\mathbf{b}} = \mathbf{3} + \mathbf{2 \cdot p} + \mathbf{4 \cdot p^2} + \dots$$