Tutorial Solutions: Week 6

Orlagh Carroll, Sile Tiernan, Ciara Moynihan, Colm O'Shaughnessy, Conor Hughes

February 23, 2014

1 Question 1

$x^2 \equiv$ a mod p^n has 2 solutions:
One solution is when p is odd and the other is when a, p are coprime.

Suppose $x^2 = y^2 \equiv a \ mod \ p^n$
$x^2 - y^2 = (x+y)(x-y) \equiv 0 \ mod \ p^n$

p^n | (x - y)(x + y) $\Rightarrow p$ | (x - y)(x + y)

If p | (x + y) and p | (x - y) $\Rightarrow$ p | $2x$ (their sum) and p | -2y (their difference)

We know $x^2 = kp^n + a$
p | x $\Rightarrow$ p | x^2 $\Rightarrow$ p | a which is not true as gcd(a,p) = 1 $\Rightarrow p \nmid x$ and $p \nmid y$

It follows p | (x + y) or p | (x - y) but not both.
Since p^n | (x + y)(x - y) $\Rightarrow p^n$ | (x + y) or p^n | (x - y) (but not both).

So we have:
x $\equiv$ y mod p^n or
-x $\equiv$ y mod p^n

2 Question 2

Find all solutions to the congruence $x^2 \equiv 2(mod 7^4)$

Let $f(x) = x^2 - 2$. Now we are looking to find x such that

$f(x) \equiv 0(mod 7^4)$

First, let us find x such that $f(x) \equiv 0(mod 7)$
The values for x that satisfy this are $x = 3, x = 4$.

Now let's check if $f\prime(x) \equiv 0(mod 7)$ in both cases.

This is not true, as $f\prime(x) = 2x$, and 2*3 = 6, 2*4 = 8, are obviously not divisible by 7. Hence we can use hensel's lemma.

We will now lift one of our answers for $x, x = 3$. We will write our new solution $x = 3 + 7K$, and we will find a solution for $f(x) \equiv 0 mod 7^2$ now. We find: $x^2 = 9 + 6 * 7k + 7^2K * 2$.

As the last term is divisible by 7^2, we can cancel it from the equation (as we are working modulo 7^2).

Taking 2 away from both sides and rearranging leaves us with:

$x^2 - 2 = (6k + 1)7$. This is divisible by 7^2 when $6k + 1$ is divisible by 7.

This is true for k = 1, so our new solution is $x = 3 + 7(1) = 10$. $f\prime(x) \neq 0(mod 7^2)$ in this case once again, so we can apply hensel's lemma once again for 7^3

Writing our new solution as $3+7+7^2k$, we find x^2 once agan and subtract two from both sides to get our $x^2 - 2$ expression.

Any expression with a coefficient of 7^3 or higher can be ignored as this will be divisible by 7^3. Simplifying we get:

$x^2 - 2 = 7^2(6k + 2)$.

This is divisible by 7^3 when 6k + 2 is divisible by 7. This true for k = 2. So our solution for x here is $x = 3 + 7 + (2)7^2$. Once again we can check the value of $f\prime(x)$ and it is not divisible by 7.

So we can apply Hensel's lemma once more.

Writing our new solution as $x = 3 + 7 + (2)7^2 + 7^3(k)$, , we wish to find x such that $f(x) \equiv 0(mod 7^4)$.

We first find: $x^2 - 2 = 7^3(6k + 6)$. This is divisibe by 7^4 when $6k + 6$ is divisible by 7. This is true for k = 6.

So our final solution for $x = 3 + 7(1) + (2)7^2 + (6)7^3 = 2166$.

The second solution for x can be found using the same proceedure except with x = 4 as the original answer, or using $x_2 = 7^4 - x_1$. Using this relation and setting $x_1 = 2166$, we get $x_2 = 235$

Solutions; $x = 2166, x = 235$

3 Question 3

Find all solutions to the congruence $x^2 \equiv -3\ mod(13^3)$.
$x^2 \equiv -3\ mod(13^3)$
$x^2 \equiv -3\ mod 13$ has solutions $x = \pm 6, x = 6, 7$
$f(x) = x^2 + 3$
$f'(x) = 2x \neq 0\ for\ x = 6, 7$ so Hensel's Lemma applies and we can lift.
$y = 6 + 13k$
$y^2 = 36 + 156k + 169k^2 \equiv (36 + 156k)\ mod(13^2)$
$y^2 + 3 \equiv (39 + 156k) \equiv 39(1 + 4k)$
so $k = 3\ \ y = 45$
$z = 45 + j13^2$
$z^2 \equiv 2025 + 15216j\ mod(13^3)$
$z^2 + 3 \equiv 2028 + 15210j\ mod(13^3)$
$j = 12$
$x = 6 + 3(13) + 12(13^2) = 2073$
The second solution for x: $x = 13^3 - 2073 = 124$

4 Question 4

Let f(x)=(x^2−2)$(x^2-17)(x^2-34)$. $p \neq 2, 17$. Therefore the gcd(2,p)=gcd(17,p)=1.
If $\left(\frac{2}{p}\right) = 1,$ then $x^2 - 2 \equiv 0 \bmod p$ has solutions..
If $\left(\frac{17}{p}\right) = 1,$ then $x^2 - 17 \equiv 0 \bmod p$ has solutions.

If $\left(\frac{34}{p}\right) = \left(\frac{17}{p}\right) = -1,$ then $\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right).$
$\left(\frac{17}{p}\right) = 1$ and $x^2 - 34 \equiv 0 \bmod p$ has solutions.
$f'(x) = 2x(x^2-2)(x^2-17) + 2x(x^2-34)(x^2-2) + 2x(x^2-17)(x^2-34).$
Therefore $f'(x) \neq 0$ because, for example, if $x^2 - 2 \equiv 0 \bmod p$
has solution x=a then a term is left over:$f'(a) = 2a(a^2-17)(a^2-34) \bmod p.$
Hence we can apply Hensel's Lemma for higher powers.

5 Question 5

For p=17, f(x)=(x$^2 - 2)(x^2-17)(x^2-34) \equiv x^4(x^2-2) \bmod 17.$
$x = 6$ is a root of $(x^2-2) \equiv 0 \bmod 17.$
$f'(6) = 2.6 \neq 0 \bmod 17.$ Hence we can then apply Hensel's Lemma.

For $p = 2,\ f(x) = x^4(x^2-17) \bmod 2$ with x=1 as a solution.
x=1 is also a solution for $f(x) \bmod 4,\ f(x) \bmod 8,\ f(x) \bmod 16$ but not for $f(x) = (x^2-2)^2(x-17) \bmod 32.$
$f(x) = (x^2-2)^2(x-17) \bmod 32$ has root $x = 7$. Therefore$f'(7) = 2 \bmod 4.$
Hence, we have found a root by Hensel's Lemma for all $n5$ and a root for n=1,2,3,4.

6 Question 6

$(x^3-37)(x^2+3), p \neq 2,3$ then x^2+3 has roots $\iff (\frac{-3}{p}) = 1$
We know that $(\frac{-3}{p}) = (\frac{p}{3})$ from last week's tutorial.

$p \equiv 1(mod 3) \implies (\frac{p}{3}) = 1 \implies (\frac{-3}{p}) = 1$
So $\exists x$ such that $x^2+3 \equiv 0(modp)$ and $x \not\equiv 0(modp)$
We can lift these roots (mod p^n) by Hensel's Lemma.

$p \not\equiv 1(mod 3) \implies x \longmapsto x^3$ on $(Z/pZ)^\times$ is injective.
$x^3 \equiv y^3(modp), x, y \in (Z/pZ)^\times$
$(xy^{-1})^3 \equiv (modp)$
xy^{-1} is of order 1 or 3, but can't be of order three, by Lagrange's Theorem
$\implies xy^{-1} = 1, x = y$ is an injective map of a finite set to itself and is therefore also surjective
so $x^3 - 37$ has roots wherever p $\not\equiv$1(mod3) and by Hensel's lemma $(x^3 - 37)(x^2+3)$ has roots in (Z/p^nZ) for all n when p$\neq$2,3.

7 Question 7

p=2
agrees with the above solution as $2 \not\equiv 1 (mod 3)$ and Hensel's Lemma applies and $(x^3 - 37)(x^2 + 3)$ has roots in $(Z/p^n Z)$ for all n when p=2.

p=3
$x^3 - 37, x = 4 : 4^3 - 37 = 64 - 37 = 3^3$
$f'(x) = 3x^2$ is only divisible by 3^1 when x=4
so once again we can apply Hensel's Lemma and conclude that $(x^3 - 37)(x^2 + 3)$ has roots in $(Z/p^n Z)$ for all n when p=3.