LECTURE NOTES: A SPECIAL CUBIC MODULO PRIMES

GERGELY HARCOS

We shall prove the following result.

Theorem. *Let $p \neq 3$ be a prime. If $p \equiv \pm 1 \pmod 9$ then $x^3 - 3x - 1$ has three distinct roots modulo p. Otherwise $x^3 - 3x - 1$ has no root modulo p.*

We need a certain amount of algebra for the proof. Observe that the residues modulo p form a set $\mathbb{F}_p$ in which the four basic operations of arithmetic can be performed (modulo p of course), and the "usual rules" apply. For example, $1/(a-b) + 1/(a+b) = 2a/(a^2 - b^2)$ for all residues such that $a \neq \pm b$. We say that $\mathbb{F}_p$ is a ***field***, it is an example of a ***finite field***. You are already familiar with some infinite fields, namely $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. If F is a field, then we can talk about polynomials $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ with coefficients a_i in F, and we can add or multiply them in the usual manner. For example in $\mathbb{F}_5$ we have $(x-2)(x+2) = x^2 + 1$ which shows that modulo 5 there exist two square-roots of -1, namely ± 2. If a polynomial with coefficients in F is a product of smaller degree polynomials, then we say it is *reducible*, otherwise we say it is *irreducible*. The irreducible polynomials play a similar role among all polynomials as primes among integers. For example, every monic polynomial can be written as a product of monic irreducible polynomials in a unique fashion apart from reordering the factors. If we are given a polynomial with *integer* coefficients, then for any prime p we can regard it as a polynomial with coefficients in $\mathbb{F}_p$ and ask how it factors into irreducibles among such polynomials. As p varies, the decomposition pattern varies greatly yet there is some regularity (e.g. statistically) in them. Understanding how and to what extent this regularity holds, turned out to be a very deep and fundamental question in number theory. A lot of current research is aimed at understanding some aspect of this general question.

Example 1. Here are factorizations of $x^5 - 8x^2 + 3$ into irreducibles modulo a few primes:

$$x^5 - 8x^2 + 3 \equiv x^2(x+1)^3 \pmod 3$$
$$x^5 - 8x^2 + 3 \equiv (x^2 + 6x + 3)(x^3 + x^2 + 5x + 1) \pmod 7$$
$$x^5 - 8x^2 + 3 \equiv (x+3)(x^2 + 3x + 10)(x^2 + 7x + 4) \pmod{13}$$
$$x^5 - 8x^2 + 3 \equiv x^5 + 15x^2 + 3 \pmod{23}$$
$$x^5 - 8x^2 + 3 \equiv (x+25)(x+26)(x^3 + 7x^2 + 8x + 22) \pmod{29}$$
$$x^5 - 8x^2 + 3 \equiv (x+16)(x+22)(x+27)(x^2 + 28x + 26) \pmod{31}$$
$$x^5 - 8x^2 + 3 \equiv (x+32)(x^4 + 21x^3 + 17x^2 + 31x + 15) \pmod{53}$$
$$x^5 - 8x^2 + 3 \equiv (x+12)(x+20)(x+40)(x+66)(x+68) \pmod{103}.$$

You can generate such examples with *MATHEMATICA*® using the following command:

```
TableForm[Table[{Prime[n],
Factor[x^5-8x^2+3,Modulus->Prime[n]]},{n,1,100}]]
```

A very important feature of fields is the following. If F is any field and $P(x)$ is any polynomial with coefficients in it, then F is contained in some field F' where $P(x)$ has a root. The construction of F' from F and $P(x)$ is similar to how we construct $\mathbb{C}$ from $\mathbb{R}$ and x^2+1. Without loss of generality, $P(x)$ is irreducible of some degree n. Then F' is simply the set of formal expressions $a_0+a_1\xi+\cdots+a_{n-1}\xi^{n-1}$ where ξ is just a symbol and the coefficients a_i are from F. It is clear how to add such expressions: we do it componentwise. The natural multiplication also works, but we might encounter powers of ξ beyond ξ^{n-1}. In this case we act as if ξ were a root of $P(x)$. The equation $P(\xi)=0$ exactly tells us how to express ξ^n as a combination of $1,\xi,\dots,\xi^{n-1}$. Using this rule repeatedly, we can express *any* power of ξ as a combination of $1,\xi,\dots,\xi^{n-1}$, hence we obtain a well-defined multiplication on our set F'. It is remarkable that F' is a field, that is, we can even divide by nonzero elements. The reason is essentially the same as why $\mathbb{F}_p$ is a field. There we need to show that for any integer q not divisible by p there are integers r,s such that $qr-ps=1$; these can be found by running the Euclidean algorithm on the pair (q,p). Here we need to show that for any polynomial $Q(x)$ not divisible by $P(x)$ there are polynomials $R(x),S(x)$ such that $Q(x)R(x)-P(x)S(x)=1$; these can be found by running the Euclidean algorithm on the pair (Q,P). In the field F' just described, ξ is indeed a root of $P(x)$!

Example 2. From Example 1 we know that x^3+x^2+5x+1 is irreducible in $\mathbb{F}_7$. Now we can "add a root" ξ of this polynomial to $\mathbb{F}_7$ by considering all $7^3=343$ expressions of the form $a_0+a_1\xi+a_2\xi^2$ with $a_0,a_1,a_2\in\mathbb{F}_7$ and performing the basic operations "with the understanding" that $\xi^3+\xi^2+5\xi+1=0$. We obtain a field of 343 elements. To see how it works, let us multiply two random elements:

$$\begin{aligned}(1+4\xi+2\xi^2)(5+6\xi+3\xi^2)&=5+5\xi+2\xi^2+3\xi^3+6\xi^4\\&=5+5\xi+2\xi^2+(3+6\xi)\xi^3\\&=5+5\xi+2\xi^2-(3+6\xi)(1+5\xi+\xi^2)\\&=2+5\xi+4\xi^2+\xi^3\\&=2+2\xi+3\xi^2-(1+5\xi+\xi^2)\\&=1+3\xi^2\end{aligned}$$

In other words, among polynomials with coefficients in $\mathbb{F}_7$, $(1+4x+2x^2)(5+6x+3x^2)$ has residue $1+3x^2$ when divided by $1+5x+x^2+x^3$. Indeed,

$$(1+4x+2x^2)(5+6x+3x^2)=(1+3x^2)+(4+6x)(1+5x+x^2+x^3).$$

Finding the reciprocal of $1+4\xi+2\xi^2$ in our field is a bit harder. For this we need to find polynomials $R(x)$, $S(x)$ such that

$$(1+4x+2x^2)R(x)=1+S(x)(1+5x+x^2+x^3).$$

The Euclidean algorithm provides $R(x)=6+2x+4x^2$ and $S(x)=5+x$, hence

$$(1+4\xi+2\xi^2)(6+2\xi+4\xi^2)=1.$$

Now we understand that any polynomial $P(x)$ with coefficients in a field F has a root ξ in some extension F' of F. This means that allowing coefficients from the extended field F' we have a factorization $P(x)=(x-\xi)Q(x)$. By induction on the degree n of $P(x)$ we can see that there is an extension F' of F such that $P(x)=\prod_{i=1}^n(x-\xi_i)$ for suitable $\xi_i\in F'$. In particular, for any prime p and any positive integer n there is a field F containing $\mathbb{F}_p$ such that $x^n-1=\prod_{i=1}^n(x-\xi_i)$ for suitable $\xi_i\in F$. Without any further assumption it may happen that the roots are not distinct, that is, $x^n-1=(x-\xi)^2Q(x)$ for some polynomial

$Q(x)$ with coefficients in F. The familiar notion of derivative from analysis can be defined formally for polynomials over any field. The Leibniz rule then implies for our situation that

$$nx^{n-1} = 2(x-\xi)Q(x) + (x-\xi)^2 Q'(x),$$

hence also that $n\xi^{n-1} = 0$. Here ξ^{n-1} is nonzero by $\xi^n = 1$, therefore n as an element of $\mathbb{F}_p$ is zero, whence n as an integer is divisible by p. We proved that the ξ_i's are all distinct when $p \nmid n$.

From now on we assume that $p \nmid n$. Then $\mathbb{F}_p$ has a (finite) field extension containing n distinct n-th roots of unity. Let ξ be an n-th root of unity, then there is a smallest positive integer m such that $\xi^m = 1$: we say that ξ is a *primitive* m-th root of unity. It is easy to see that $m \mid n$, hence each n-th root of unity is a primitive m-th root of unity for a unique divisor $m \mid n$. We now show by induction on n that whenever a field F contains n distinct n-th roots of unity, it contains $\varphi(n)$ primitive n-th roots of unity. If the statement holds for $m \mid n$ excluding $m = n$, then the number of nonprimitive n-th roots of unity in F is the sum of $\varphi(m)$ over these m's. This sum is $n - \varphi(n)$, hence indeed F contains $\varphi(n)$ primitive n-th roots of unity. If ξ is any of them, then $\{1, \xi, \ldots, \xi^{n-1}\}$ is the set of all n-th roots of unity and $\{\xi^k : (k,n) = 1\}$ is the set of primitive ones.

We can finally begin the proof of our Theorem. We specify $n = 9$, then $p \nmid n$ by $p \neq 3$. We shall work in a field F which contains $\mathbb{F}_p$ and a primitive 9-th root of unity ξ. Using the relations (which follow from $\xi^9 = 1$, $\xi^3 \neq 1$)

$$1 + \xi^3 + \xi^{-3} = 0 \qquad \text{and} \qquad 1 + \sum_{i=1}^{4} (\xi^i + \xi^{-i}) = 0,$$

it is straightforward to verify that

$$x^3 - 3x - 1 = (x + \xi + \xi^{-1})(x + \xi^2 + \xi^{-2})(x + \xi^4 + \xi^{-4})$$

and the factors on the right hand side are distinct. For example, $\xi + \xi^{-1} = \xi^2 + \xi^{-2}$ implies by squaring $\xi^2 + \xi^{-2} = \xi^4 + \xi^{-4}$, hence also that these all vanish because we can divide by 3 in F. But $\xi + \xi^{-1} = 0$ would yield $\xi^4 = 1$, a contradiction. Now the question boils down to the following: how many of the elements $\xi + \xi^{-1}$, $\xi^2 + \xi^{-2}$, $\xi^4 + \xi^{-4}$ lie in $\mathbb{F}_p$? To answer this, we observe that $\mathbb{F}_p$ can be identified as the set of roots of $x^p - x$ in F. Indeed, $\mathbb{F}_p$ is a subset of the roots by Fermat's little theorem but this subset already has p elements. So what we really want to know is this: how many of the elements $\xi + \xi^{-1}$, $\xi^2 + \xi^{-2}$, $\xi^4 + \xi^{-4}$ are fixed by the map $x \mapsto x^p$? This map is called the *Frobenius map* and is extremely important in number theory and algebraic geometry. It has the nice property that $(a+b)^p = a^p + b^p$ for any $a, b \in F$ by the binomial theorem. In particular,

$$(\xi + \xi^{-1})^p = \xi^p + \xi^{-p}, \quad (\xi^2 + \xi^{-2})^p = \xi^{2p} + \xi^{-2p}, \quad (\xi^4 + \xi^{-4})^p = \xi^{4p} + \xi^{-4p}.$$

Now we can see that for $p \equiv \pm 1 \pmod 9$ the Frobenius map fixes all the sums on the left hand sides, while for $p \equiv \pm 2, \pm 4 \pmod 9$ it permutes them in a cyclic fashion. The Theorem is proved.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, POB 127, BUDAPEST H-1364, HUNGARY

E-mail address: gharcos@renyi.hu