MATH 371 – Class notes/outline – October 15, 2013

More on polynomials

We now consider polynomials with coefficients in rings (not just fields) other than $\mathbb{R}$ and $\mathbb{C}$. (Our rings continue to be commutative and have multiplicative identities).

The formal definition of a polynomial p with coefficients in a ring R is that it is a function $p\colon \mathbb{N} \to R$ such that $p(n) = 0$ for all but finitely many n. We tend to write p_n rather than $p(n)$, and instead of writing $(p_0, p_1, \ldots)$ we write $p_0 + p + 1x + p_2x^2 + p_3x^3 + \cdots$. So x is the function $(0, 1, 0, 0, \ldots)$, x^2 is the function $(0, 0, 1, 0, 0, \ldots)$ and we can identify an element r of R with the function $(r, 0, 0, 0, \ldots)$. Given two polynomials p and q we form $p + q$ by letting $(p + q)(n) = (p + q)_n = p_n + q_n$ and

$$(pq)(n) = (pq)n = \sum_{i=0}^{n} p_i q_{n-i}.$$

In this way we make the ring of polynomials (in one variable) with coefficients in R into a ring, denoted $R[x]$. The *degree* of a polynomial p is the largest value of n for which $p_n \neq 0$, the *leading coefficient* is p_n, and the *leading term* of p is p_nx^n. Two polynomials p and q are equal if and only if $p(n) = q(n)$ for all $n \geqslant 0$. There is a natural inclusion $R \to R[x]$ that sends $r \in R$ to the constant polynomial r — this is a ring homomorphism.

There's some weirdness that can happen for polynomials with coefficients in an arbitrary commutative ring R. For instance, let $R = \mathbb{Z}/\langle 4\rangle$ and consider $p = q = 2x + 1$. Then $\deg(p) = \deg(q) = 2$ but $pq = 1$ in this ring, so $\deg(pq) = 0$. But if the leading coefficient of p or q is not a zero divisor then

$$\deg(pq) = \deg(p) + \deg(q).$$

Also, if R is an integral domain, then $R[x]^* = R^*$ (where we identify R with the polynomials of degree zero in $R[x]$).

Just as we have to be careful with the degree of a product, we have to be a little bit careful with the division algorithm. The most general statement one can make is that if the leading coefficient of the polynomial $d \in R[x]$ is not a zero-divisor, then given $f \in R[x]$, there exist polynomials $q, r \in R[x]$ such that

$$f = qd + r$$

where either $r = 0$ or none of the terms in r is divisible by the leading term of d. Note the care with which we have to say this, and the odd things that can happen in the division algorithm, which now goes as follows:

1. Given f and d, where the leading coefficient d_n of d is not a zero divisor, begin by setting $q = 0$, $r = 0$ and $s = f$. Note that $f = qd + (r + s)$.
2. If $s = 0$, then we're done, output q and r.
3. Let s_mx^m be the leading term of s.
4. If d_nx^n divides s_mx^m, then $m \geqslant n$ and $s_m = cd_n$ for a unique $c \in R$ and so $s_mx^m = (cx^{m-n})(d_nx^n)$. In this case, put $q := q + cx^{m-n}$ and $s := x - (cx^{m-n}d)$.

5. On the other hand, of $d_n x^n$ does not divide $s_m x^m$, then put $r := r + s_m x^m$ and $s := s - s_m x^m$.
6. After all of this, we still have $f = qd + (r + s)$.
7. Go pack to step 2.

Because the degree of s decreases each time through the loop, the process will stop after at most $\deg(s) + 1$ times and yield the result described above.

If the leading coefficient of d is a unit in R, then we have the standard result that $f = qd + r$ with $\deg(r) < \deg(d)$. Note that this is true for *monic* polynomials (leading coefficient is 1) and that a monic polynomial of degree $\geqslant 1$ is *never* a unit in $R[x]$ (proof?).

Roots. Given any $\rho \in R$, we have the *evaluation homomorphism* $\varphi_\rho \colon R[x] \to R$ (note which way it goes):

$$\varphi_\rho(p) = p(\rho) = p_0 + p_1\rho + \cdots + p_n\rho^n.$$

Borrow the notation from affine varieties and set $V(p) = \{\rho \in R \mid p(\rho) = 0\}$ to be the set of *roots* of $p \in R[x]$. We have that $\rho \in R$ is a root of $p \in R[x]$ if and only if $x - \rho$ divides p. (The proof uses the division algorithm to write $p = q(x - \rho) + r$ with $\deg(r) = 0$, i.e., $r \in R$, so $p(\rho) = r$ and ρ is a root if and only if $r = 0$, i.e., $(x - \rho) \mid p$.) The *multiplicity* of a root ρ of p is denoted $\nu_\rho(p)$ and is the largest value of n such that $(x - \rho)^n \mid p$.

A little weirdness: Let $R = \mathbb{Z}/\langle 6\rangle$ and let $p = x^2 + 3x + 2 \in R[x]$. Here's a table of $p(\rho)$ for $\rho \in R$:

ρ	0	1	2	3	4	5
$p(\rho)$	2	0	0	2	0	0

So $V(p) = \{1, 2, 4, 5\}$ and p has four roots even though its degree is only 2. It's certainly not true that $p = (x-1)(x-2)(x-4)(x-5)$, although $p = (x-1)(x-2) = (x-4)(x-5)$ (since $3 = -3$ in R etc).

On the other hand, if R is an integral domain, and $p, q \in R[x]$ then $V(pq) = V(p) \cup V(q)$. This in turn implies that if $p \neq 0$ and $V(p) = \{\rho_1, \ldots, \rho_s\}$ then

$$p(x) = Q(x)(x - \rho_1)^{\nu_{\rho_1}(p)} \cdots (x - \rho_s)^{\nu_{\rho_s}(p)},$$

where $Q \in R[x]$ and $V(Q) = \varnothing$. The number of roots of p, counted with multiplicities, is bounded by the degree of p. (Prove this by induction on the degree of p).

An interesting example: Consider the polynomial $x^p - x \in \mathbb{F}_p[x]$. Then $V(x^p - x) = \mathbb{F}_p$ by Fermat's little theorem, therefore

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1))$$

in $\mathbb{F}_p[x]$. Compare the coefficients of degree 1 on both sides and get $(p-1)! = -1$ in $\mathbb{F}_p$, which gives another (easier? more natural?) proof of Wilson's theorem.

Derivatives: In the context of a general commutative ring R, we can't use calculus (limits and such) to define the derivative of a polynomial. But we can just appropriate the formula from there, and define $p' = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$ if $p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then you can formally prove the sum and product rules for derivatives.

It's easy to prove that if $p^2 \mid q$ then $p \mid q'$ and an element $\rho \in R$ is a multiple root of p (i.e., $\nu_\rho(p) > 1$) if and only if ρ is a root of both p and p'.

One fact about derivatives that doesn't carry over from calculus is the mean-value theorem. So there are non-constant polynomials with derivative zero – for instance $q = x^p \in \mathbb{F}_p[x]$.

Cyclotomic polynomials: Let's go back to $\mathbb{C}[x]$ for a bit and consider the "nth roots of unity", i.e., the complex numbers ξ that satisfy $\xi^n = 1$. As is well known, the nth roots of unity are $\xi = e^{2\pi ki/n}$ for $k = 0, 1, \ldots, n-1$. The number ξ is called a *primitive* nth root of unity if $\xi^n = 1$ but $\xi^k \neq 1$ for $0 < k < n$. We have that $e^{2\pi ki/n}$ is a primitive nth root of unity if and only if $\gcd(k, n) = 1$. Thus there are $\varphi(n)$ primitive nth roots of unity (where φ is Euler's φ-function). Moreover, if ζ is a primitive nth root of unity and $\zeta^m = 1$. then $n \mid m$ (because then $e^{2\pi mki/n} = 1$ so mk/n is an integer; $n \mid mk$ and $\gcd(k, n) = 1$ implies $n \mid m$).

The nth *cyclotomic polynomial* $\Phi_n(x)$ is defined to be the monic polynomial whose roots are precisely the primitive nth roots of unity. So

$$\Phi_n(x) = \prod_{1 \leqslant k \leqslant n,\ \gcd(k,n)=1} (x - e^{2\pi ki/n}).$$

The first few Φ_n are

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= \left(x - \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right)\left(x - \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right) = x^2 + x + 1 \\
\Phi_4(x) &= (x - i)(x + i) = x^2 + 1
\end{aligned}$$

It is remarkable that the cyclotomic polynomials seem to (and do) all have integer coefficients, which allows us to define them as polynomials over any ring, and the following is true:

Proposition: For all $n \geqslant 1$, (i) $x^n - 1 = \prod_{d|n} \Phi_d(x)$, and (ii) $\Phi_n(x) \in \mathbb{Z}[x]$, i,e., the cyclotomic polynomials have integer coefficients.

Proof. The roots of $x^n - 1$ are all the nth roots of unity. The roots of the $\Phi_d(x)$ are the primitive dth roots of unity, where $d \mid n$, so all the roots of the product on the right side of (i) are roots of $x^n - 1$. But each root of $x^n - 1$ must be a primitive dth root of unity for some $d \leqslant n$ for which $d \mid n$. Thus the polynomials on the left and right sides of (i) have the same roots, and they are both monic, so they are equal (since $\mathbb{C}$ is a field). To prove $\Phi_n(x) \in \mathbb{Z}[x]$ we use induction on n. We know the first few cases are true. For $n > 1$, set $f = \prod_{d<n,\ d|n} \Phi_d$, so that $x^n - 1 = \Phi_n f$. By induction (since f is the product of Φ_d's for $d < n$), we know that f is a monic integer polynomial. Division of polynomials in $\mathbb{Z}[x]$ gives $x^n - 1 = qf + r$ where $r = 0$ or $\deg(r) < \deg(f)$ and $q \in \mathbb{Z}[x]$. Since f is monic, we have that q and r are unique in $\mathbb{Z}[x]$ as well as in $\mathbb{C}[x]$, so we must have $q = \Phi_n$ and $r = 0$. Therefore $\Phi_n = q \in \mathbb{Z}[x]$.

The identity (i) above is true in any $R[x]$, via the canonical homomorphism from $\mathbb{Z}$ to R, extended to be a homomorphism from $\mathbb{Z}[x]$ to $R[x]$. So we generalize the notion of *primitive nth root of unity* to any commutative ring R: $\alpha \in R$ is a primitive nth root of unity if $\alpha^n = 1$ and $\alpha^k \neq 1$ for $1 \leqslant k < n$.

Lemma: Suppose R is an integral domain, and let $\alpha \in R$. If $\Phi_n(\alpha) = 0$ and if α is *not* a multiple root of $x^n - 1 \in R[x]$, then α is a primitive nth root of unity in R.

Proof. The identity $x^n - 1 = \prod_{d|n} \Phi_d(x)$ in $R[x]$ means there is a factorization $q\Phi_n = x^n - 1$ for some $q \in R[x]$. Therefore $\alpha^n - 1 = q(\alpha)\Phi_n(\alpha) = 0$ and so $\alpha^n = 1$. If α is a primitive dth root of unity for some $1 \leqslant d < n$, then we must have $d \mid n$ by the parenthetical remark above. In this case, we have $x^n - 1 = \prod_{c|d} \Phi_c(x)$ by (i) again, and since R is an integral domain we'll have $\Phi_c(\alpha) = 0$ for some $c \mid d$. But now α is a root of at least two of the factors in $x^n - 1 = \prod_{d|n} \Phi_d(x)$, namely Φ_n and Φ_c for some $c \leqslant d < n$, so α is a multiple root of $x^n - 1$, a contradiction.

Using this lemma, we can prove an important result due to Gauss:

Theorem: Let F be a field and let $G \subset F^*$ be a finite subgroup of the group of units in F. Then G is cyclic.

Proof. Let $N = |G|$ and consider the polynomial $x^N - 1 = \prod_{d|N} \Phi_d(x) \in F[x]$. The roots of $x^N - 1$ are precisely the elements of G, since every element of G is a root, and there are at most N, and hence exactly N such roots. This tells us that none of the roots of $x^N - 1$ are multiple roots. But then Φ_N must have $\deg(\Phi_N) = \varphi(N)$ roots, which are primitive Nth roots of unity by the lemma above, and hence are generators of G.

A corollary of this theorem is that $\mathbb{F}_p^*$ is a cyclic group. An integer a such that $[a]$ generates $\mathbb{F}_p^*$ is called a *primitive root* mod p. For instance, 2 is a primitive root mod 13 (try it!). There doesn't seem to be any way to identify the $\varphi(p-1)$ primitive roots among the elements of $\mathbb{F}_p^*$ (the proportion of them can be arbitrarily small).

Another application of cyclotomic polynomials:

Theorem: There are infinitely many prime numbers $\equiv 1 \pmod{n}$ for any $n \geqslant 2$.

Proof. It is enough to show that there exists a prime number $\equiv 1 \pmod{n}$ for every $n \geqslant 2$ (why?). From the definition of Φ_n, we have for $n \geqslant 2$ that $|\Phi_n(n)| > 1$. So there is a prime p such that $p \mid \Phi_n(n)$. Now the constant term of Φ_n is ± 1 since $|\Phi_n(0)| = 1$ and $\Phi_n(0) \in \mathbb{Z}$, which shows that $p \nmid n$ (since if $p \mid n$ then p would divide every term of $\Phi_n(n)$ except the constant term 1, but we're assuming $p \mid \Phi_n(n)$). Therefore $[n]$ is not a multiple root of $x^n - 1 \in \mathbb{F}_p[x]$ (since p does not divide the derivative of $x^n - 1$ evaluated at $x = n$). Since $\Phi_n([n]) = 0$ in $\mathbb{F}_p$, this implies by the lemma above that the order of $[n]$ is n in $\mathbb{F}_p^*$. Therefore n divides $|\mathbb{F}_p| = p - 1$ and so $p \equiv 1 \pmod{n}$.

More on ideals in polynomial rings. We already know that if F is a field, then $F[x]$ is a Euclidean domain (the degree of a polynomial is the Euclidean function). Therefore $F[x]$ is a principal ideal domain and a unique factorization domain and the division algorithm works in $F[x]$

We illustrate this by finding $\gcd(x^5 + x + 1\,,\, x^4 + x^3 + x + 1)$ in $\mathbb{F}_2[x]$.

i	-1	0	1	2	3
r_i	$x^5 + x + 1$	$x^4 + x^3 + x + 1$	$x^3 + x^2 + x$	$x^2 + x + 1$	0
q_i	$-$	$-$	$x + 1$	x	x
λ_i	1	0	1	x	$-$
μ_i	0	1	$x + 1$	$x^2 + x + 1$	$-$

So the gcd is $x^2 + x + 1$ and $x^2 + x + 1 = x(x^5 + x + 1) + (x^2 + x + 1)(x^4 + x^3 + x + 1)$ in $\mathbb{F}_2[x]$.

Recall that the units in $F[x]$ are the non-zero constants, and if p is not irreducible then there are polynomials q_1 and q_2 such that $p = q_1 q_2$ and $0 < \deg(q_1), \deg(q_2) < \deg(p)$. So the following are direct consequences of things we already know:

Proposition: For $p \in F[x]$,
(i) The ideal $\langle p \rangle$ is maximal if and only if p is irreducible, in which case $F[x]/\langle p \rangle$ is a field.
(ii) p is a unit if and only if $\deg(p) = 0$.
(iii) If $\deg(p) = 1$ then p is irreducible (and $F[x]/\langle p \rangle \cong F$).
(iv) If p is irreducible and $\deg(p) > 1$ then p does not have any roots.
(v) If $\deg(p) = 2$ or 3 then p is irreducible if and only if it has no roots.

Examples: The polynomial $p = x^3 + x + 1 \in \mathbb{F}_5[x]$ is irreducible since it is degree 3 and has no roots:

x	0	1	2	3	4
$p(x)$	1	3	1	1	4

But $q = x^4 + x^2 + 1 \in \mathbb{F}_2[x]$ has no roots since $q(0) = 1$ and $q(1) = 1$, but $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ in $\mathbb{F}_2[x]$.

Gauss proved (and we might prove one of these days) that the cyclotomic polynomials are irreducible in $\mathbb{Q}[x]$. In the homework we'll explore which cyclotomic polynomials Φ_n are irreducible in $\mathbb{F}_p[x]$.

In Galois theory, one studies the situation where there is a field F and a polynomial $p \in F[x]$ with no roots in F, along with an extension field $E \supset F$ containing an element α for which $p(\alpha) = 0$ (we view p also as an element of $E[x]$). The most familiar case of this is $F = \mathbb{R}$, $E = \mathbb{C}$, $p = x^2 + 1$ and $\alpha = i$. There is a natural construction of such an E, given F and p. For instance $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$.

Because it's really no harder, we'll do this construction in the general case $R[x]$ where the coefficients come from a ring that is not necessarily a field. First a remark: Suppose I is an ideal in $R[x]$ such that $R \cap I = \langle 0 \rangle$ (where we consider R to be the subring of constant polynomials in $R[x]$, so the only constant polynomial in I is the zero polynomial). If $r_1, r_2 \in R$ and $[r_1] = [r_2] \in R/I$, then $r_1 - r_2 \in R \cap I$ and so $r_1 = r_2$. So if $R \cap I = \langle 0 \rangle$ we can simply write r to denote the element $[r]$ in $R[x]/I$.

Proposition: Let R be a ring and

$$p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$$

be a *monic* polynomial of degree n. Then $R \cap \langle p \rangle = \langle 0 \rangle$. Each element $[q] = q + \langle p \rangle$ in the quotient ring $R[x]/\langle p \rangle$ can be expressed uniquely as a polynomial of degree less than n in $[x]$: $b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$, where $b_0, \ldots, b_{n-1} \in R$ and $\alpha = [x]$. In $R[x]/\langle p \rangle$ we have the identity

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0 .$$

It is essential that p is a monic polynomial so that the considerations about degree on page 1 of these notes apply. Note that the natural ring homomorphism $\varphi\colon R \to R[x]/\langle p \rangle$ given by $\varphi(r) = [r]$ is injective, so we can view R as a subring of $R[x]/\langle p \rangle$.

In the special case that $R = F$, a field and p is an irreducible polynomial, then $\langle p \rangle$ is a maximal ideal and $F[x]/\langle p \rangle$ is an extension field E of F, and $\alpha = [x] \in E$ is actually a root of p.

Example. Let $p = x^2 + x + 1 \in \mathbb{F}_2[x]$, which is irreducible since it has no roots. By the proposition, the quotient ring $E = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ is a field, whose elements are of the form $a + b\alpha$, where $a, b \in \mathbb{F}_2$ and $\alpha^2 = -1 - \alpha = 1 + \alpha$ determines the multiplication rule:

$$(a + b\alpha)(c + d\alpha) = ac + (ad + bc)\alpha + bd\alpha^2 = (ac - bd) + (ad + bc - bd)\alpha$$

(it doesn't matter whether we use plus or minus signs since the characteristic of the field is 2). Note that E is an extension field of $\mathbb{F}_2$ having 4 elements.

The law of quadratic reciprocity. Before the break, we were concerned with which in $\mathbb{F}_p$ are quadratic residues, i.e., which half of the non-zero elements of $\mathbb{F}_p$ can be expressed as the squares of elements of $\mathbb{F}_p$. We introduced the *Legendre symbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Recall that the Legendre symbol satisfies

$$\left(\frac{a}{p}\right) = \left(\frac{a + kp}{p}\right)$$

for any $k \in \mathbb{Z}$, and if p is an odd prime and a is an integer not divisible by p, then we have Euler's formula

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

This allows us to conclude that if p is an odd prime, then the Legendre symbols satisfy:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

and we noted that

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

tells us that if p is an odd prime, then -1 is a quadratic residue mod p if $p \equiv 1 \pmod 4$ and -1 is a quadratic non-residue mod p if $p \equiv 3 \pmod 4$.

We can get a little more information in an elementary way by following in Gauss's footsteps. We start as follows: For odd primes p, we're used to writing the numbers in $\mathbb{F}_p$ as $0, 1, \ldots, p-1$, but we could just as easily write them as

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{p-3}{2}, \frac{p-1}{2}.$$

For any integer a such that $p \nmid a$, we consider the list of numbers

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a.$$

None of these numbers is divisible by p, and no pair of these are congruent to each other mod p. We set $\mu_p(a)$ (or just $\mu(a)$ if p is clear from the context) equal to the number of elements of this list that are congruent to negative numbers in the above listing of $\mathbb{F}_p$ (or to numbers bigger than $p/2$ in the standard listing of $\mathbb{F}_p$). For instance, if $p = 11$ then $\mu(6) = 3$, since $6, 12, 18, 24, 30$ are congruent to $-5, 1, -4, 2, -3$ mod 11. Using the μ function, we can give another characterization of Legendre symbols:

Lemma (Gauss): With the above notation, if $p \nmid a$, then $\left(\frac{a}{p}\right) = (-1)^{\mu_p(a)}$.

Idea of proof: Each number ka for $k = 1, \ldots, (p-1)/2$ is congruent to $\pm m_k$ for $1 \leqslant m_k \leqslant (p-1)/2$. When $1 \leqslant j, k \leqslant (p-1)/2$ and $j \neq k$, we cannot have $ja \equiv \pm ka \pmod{p}$ (since $\mathbb{F}_p$ is a field), and by the definition of μ we conclude that

$$a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv (-1)^{\mu_p(a)}\left(\frac{p-1}{2}\right)! \pmod{p}$$

and so Gauss's result follows from Euler's after canceling off the $((p-1)/2)!$.

Using this, we can determine when 2 is a quadratic residue mod p for p an odd prime. Namely, 2 is a quadratic residue mod p of $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$, and 2 is a quadratic non-residue mod p if $p \equiv 3, 5 \pmod 8$. To see this, we need to compute $\mu_p(2)$, i.e., how many of the numbers $2, 4, \ldots, p-1$ are greater than $p/2$. And if $p \equiv 1 \pmod 4$ then this number is $(p-1)/4$, where if $p \equiv 3 \pmod 4$ it's $(p+1)/4$. Therefore

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8 \\ 1 & \text{if } p \equiv 7 \pmod 8 \end{cases}$$

To do much more, we need the powerful law of quadratic reciprocity, due to Gauss. It states that if p and q are odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Another way to say this is

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{q}{p}\right) & \text{otherwise} \end{cases}$$

It is remarkable that the two congruences

$$x^2 \equiv q \pmod{p} \quad \text{and} \quad x^2 \equiv p \pmod{q}$$

should have any connection. But here's an example that shows the usefulness of the law of quadratic reciprocity in computing Legendre symbols:

$$\left(\frac{19}{43}\right) = -\left(\frac{43}{19}\right) = -\left(\frac{5}{19}\right) = -\left(\frac{19}{5}\right) = -\left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = -1$$

and so the congruence $x^2 \equiv 19 \pmod{43}$ has no solutions.

To prove Gauss's law of quadratic reciprocity we will work in the ring

$$R = \mathbb{F}_p[x]/\langle 1 + x + \cdots + x^{q-1} \rangle.$$

From the proposition on page 5, an element in R can be written uniquely in terms of $\alpha = [x]$ as

$$c_0 + c_1\alpha + \cdots + c_{q-1}\alpha^{q-2}$$

where $c_0, \ldots, c_{q-2} \in \mathbb{F}_p$.

Lemma: The element α is a primitive qth root of unity in R. Moreover, if $q \nmid \ell$ and $\beta = \alpha^\ell$ then

$$1 + \beta + \cdots + \beta^{q-1} = 0$$

in R.

Proof. We know from the proposition that $\alpha, \alpha^2, \ldots, \alpha^{q-2} \neq 1$ and $\alpha^{q-1} = -1 - \alpha - \cdots - \alpha^{q-2} \neq 1$. But $\alpha^q = \alpha\alpha^{q-1} = 1$, and so α is a primitive qth root of unity. If $q \nmid \ell$ then $\gcd(q, \ell) = 1$, and so $\{1, \alpha, \ldots, \alpha^{q-1}\} = \{1, \beta, \ldots, \beta^{q-1}\}$, which gives the equation in the lemma.

Gauss sums. We define the *Gauss sum* in R to be

$$G = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \alpha^k.$$

Because we're working in R (where $\alpha^q = 1$), the individual terms satisfy

$$\left(\frac{k}{q}\right) \alpha^k = \left(\frac{k+qm}{q}\right) \alpha^{k+qm}$$

for every $m \in \mathbb{Z}$. We'll use this often to prove two important properties of G:

1. $G^2 = (-1)^{(q-1)/2} q$.
2. If $q \neq p$, then G is an invertible element in the ring R.

Proof. The invertibility of G follows from (1) since $q \in \mathbb{F}_p \subset R$ is invertible in R since it is invertible in $\mathbb{F}_p$ for $q \neq p$. To prove (1), we start calculating:

$$\begin{aligned} G^2 &= \left(\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \alpha^k\right) \left(\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \alpha^k\right) \\ &= \left(\sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \alpha^j\right) \left(\sum_{k=1}^{q-1} \left(\frac{-k}{q}\right) \alpha^{-k}\right) \end{aligned}$$

(where we reversed the second sum and used that $\left(\frac{q-k}{q}\right) \alpha^{q-k} = \left(\frac{-k}{q}\right) \alpha^{-k}$). Next,

$$\begin{aligned} G^2 &= \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{j}{q}\right) \left(\frac{-k}{q}\right) \alpha^{j-k} \\ &= \left(\frac{-1}{q}\right) \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{jk}{q}\right) \alpha^{j-k} \\ &= (-1)^{(q-1)/2} \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{j^2 k}{q}\right) \alpha^{j(1-k)} \end{aligned}$$

where in the last equality we used the fact about $\left(\frac{-1}{p}\right)$ from near the bottom of page 6 and we replaced k with jk, since as k runs through $1, \ldots, q-1$ the remainders of jk mod q also run through $1, \ldots, q$ (though not necessarily in the same order). Since $\left(\frac{j^2}{q}\right) = 1$ by definition, we get

$$\begin{aligned} G^2 &= (-1)^{(q-1)/2} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{j=1}^{q-1} \alpha^{j(1-k)} \\ &= (-1)^{(q-1)/2} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{j=0}^{q-1} \alpha^{j(1-k)} \end{aligned}$$

because $\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) = 0$ (half the numbers between 1 and $q-1$ are quadratic residues mod q). From the lemma above, we have that $\sum_{j=0}^{q-1} \alpha^{j(1-k)} = 0$ unless $k = 1$, in which case the sum is q. This gives the formula for G^2 in (1) above.

Proof of the law of quadratic reciprocity. Raise G to the pth power in R and get

$$\begin{aligned} G^p &= (G^2)^{(p-1)/2} G = (-1)^{(p-1)(q-1)/4} q^{(p-1)/2} G \\ &= (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right) G \end{aligned}$$

using Euler's formula for the Legendre symbol. On the other hand, we can calculate G^p from the definition and use the "freshman dream" in the ring R to get

$$\begin{aligned} G^p &= \left(\sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \alpha^j\right)^p = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \alpha^{pj} \\ &= \sum_{j=1}^{q-1} \left(\frac{p}{q}\right) \left(\frac{pj}{q}\right) \alpha^{pj} = \left(\frac{p}{q}\right) G \end{aligned}$$

Since G is invertible, we can cancel G from the two expressions for G^p and get the law of quadratic reciprocity:

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).$$

The above is one of the half-dozen or so proofs that Gauss gave of the law of quadratic reciprocity. He was so taken with the theorem that he called it his "Theorema Aureum".

Finite fields.

Next we turn to the remarkable fact that for every prime p and every $n \geqslant 1$ there exists a unique field with p^n elements (we constructed a field with 2^2 elements above).

Lemma: Suppose F is a finite field, then $|F| = p^n$, where p is a prime number, $n \geqslant 1$, and there exists an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree n such that $F \cong \mathbb{F}_p[x]/\langle f \rangle$.

Proof. Start with the unique ring homomorphism $\kappa\colon \mathbb{Z} \to F$, which is not injective since F is finite. Therefore the characteristic (generator of the kernel of κ) of F is a prime number p and $\mathbb{F}_p$, being the image of κ, is a subring of F. By the first theorem on page 4, we have that F^* is a cyclic group, so let σ be a generator of F^*. Thus, every element in F is either 0 or else some power σ^n of σ. Since $\varphi_\sigma(x) = \sigma$, and so $\varphi_\sigma(x^n) = \sigma^n$, the ring homomorphism $\varphi_\sigma\colon F[x] \to F$ is surjective, and in fact, since $x \in \mathbb{F}_p[x] \subseteq F[x]$, we can restrict φ_σ to $\mathbb{F}_p[x]$ and get a surjective homomorphism

$$\varphi\colon \mathbb{F}_p[x] \to F.$$

The kernel of φ is a principal ideal $\langle f\rangle \subset \mathbb{F}_p[x]$, and $\mathbb{F}_p[x]/\langle f\rangle \cong F$, so $\langle f\rangle$ is a maximal ideal. Therefore f is an irreducible polynomial (by (i) of the Proposition on page 5). And $|F| = p^n$, where $n = \deg(f)$ by the other proposition on page 5.

Our goal now is to prove the main result of this subsection:

Theorem: There exists a finite field with p^n elements, where p is a prime number and $n \geqslant 1$. More precisely:

(i) There exists an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n.
(ii) If F and F' are finite fields with p^n elements, then there is a ring isomorphism $F \to F'$.

Proof. To prove (i), we are going to use cyclotomic polynomials — since the cyclotomic polynomial Φ_k has integer coefficients, we can use the homomorphism $\kappa\colon \mathbb{Z} \to \mathbb{F}_p$ to consider Φ_k as an element of $\mathbb{F}_p[x]$. We are going to show that if f is an irreducible polynomial dividing Φ_{p^n-1} in $\mathbb{F}_p[x]$, then $\deg(f) = n$.

To do this, suppose $\deg(f) = d$, then we know that $E = \mathbb{F}_p[x]/\langle f\rangle$ is a field with p^d elements and $\alpha = [x]$ is a root of $f \in \mathbb{F}_p[x] \subset E[x]$. Since $f \mid \Phi_{p^n-1}$ we have $gf = \Phi_{p^n-1}$ for some $g \in \mathbb{F}_p[x]$ and we get that $\Phi_{p^n-1}(\alpha) = g(\alpha)f(\alpha) = 0$. The derivative of $x^{p^n-1} - 1 \in \mathbb{F}_p[x]$ is $-x^{p^n-2}$, therefore α is not a multiple root of $x^{p^n} - 1$ and so α is a primitive $(p^n - 1)$th root of unity. But $\alpha^{p^d-1} = 1$ (that's the order of the group E^*), and so $p^n - 1 \mid p^d - 1$.

On the other hand, let $R = \{\xi \in E \,|\, \xi^{p^n} = \xi\}$, which is a subring of E (use the freshman dream to get additivity). Since $\alpha^{p^n-1} = 1$, we must have $\alpha \in R$, and since $E = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \,|\, a_i \in \mathbb{F}_p\}$, it follows that $R = E$ (since R contains 1 and all powers of α and is a subring of E). Now we know there is a primitive $(p^d - 1)$th root of unity ζ in E, and since $E = R$ we have $\zeta \in R$ and so $\zeta^{p^n-1} = 1$. But then $p^d - 1 \mid p^n - 1$ and combining this with the preceding paragraph tell us that $p^d - 1 = p^n - 1$, or $d = n$. This completes the proof of (i).

To prove (ii), suppose F and F' are finite fields with p^n elements. By the lemma above, $F \cong \mathbb{F}_p[x]/\langle f\rangle$ for some irreducible polynomial f of degree n, and $f(\alpha) = 0$, where $\alpha = [x] \in F$. The set $I = \{g \in \mathbb{F}_p[x] \,|\, g(\alpha) = 0\} \subsetneq \mathbb{F}_p[x]$ is an ideal in $\mathbb{F}_p[x]$, and $f \in I$. Therefore $\langle f\rangle \subset I$, but $\langle f\rangle$ is a maximal ideal (because F is a field) and so $I = \langle f\rangle$.

Now F^* is a finite group with $p^n - 1$ elements, therefore $\beta^{p^n-1} - 1 = 0$ for every $\beta \in F^*$, which implies that $x^{p^n} - x \in I$ and therefore $f \mid x^{p^n} - x$ in $\mathbb{F}_p[x]$. On the other hand, in $F'[x]$ we have that

$$x^{p^n} - x = \prod_{\gamma \in F'} (x - \gamma),$$

since every $\gamma \in F'$ satisfies $\gamma^{p^n} - \gamma = 0$ as well. Therefore $f \in \mathbb{F}_p[x] \subset F'[x]$ must have a root $\alpha' \in F'$ since f divides $x^{p^n} - x$. So consider the ring homomorphism

$$\varphi_{\alpha'} : \mathbb{F}_p[x] \to F'.$$

Chearly $\langle f \rangle \subset \ker(\varphi_{\alpha'})$, but since $\ker(\varphi_{\alpha'})$ is a proper ideal and $\langle f \rangle$ is a maximal ideal in $\mathbb{F}_p[x]$, we must have $\langle f \rangle = \ker(\varphi_{\alpha'})$. Therefore there is an injective ring homomorphism

$$\mathbb{F}_p[x]/\langle f \rangle \to F'$$

which must also be surjective since F' has the same number of elements as $\mathbb{F}_p[x]/\langle f \rangle \cong F$. Thus $F \cong F'$ and we are done.

We know that $x^{p^n} - x = x(x^{p^n-1} - 1) = x \prod_{d \mid p^n-1} \Phi_d$ in $\mathbb{F}_p[x]$. And by the theorem on the preceding page, we know that $x^{p^n} - x$ is divisible by an irreducible polynomial of degree n. But we can say a bit more about this, in particular we can calculate the complete irreducible factorization of $x^{p^n} - x$ in $\mathbb{F}_p[x]$. For instance in $\mathbb{F}_2[x]$,

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

and in $\mathbb{F}_3[x]$,

$$x^{3^2} - x = x^9 - x = x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2).$$

In general we have the following:

Theorem. The polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$ is the product $x^{p^n} - x = f_1 f_2 \cdots f_k$ of *all* the monic irreducible polynomials $f_1, \ldots, f_k$ in $\mathbb{F}_p[x]$ of all degrees d for which $1 \leqslant d \leqslant n$ and $d \mid n$.

Proof. We can restate the theorem as follows: For d such that $1 \leqslant d \leqslant n$ and $f \in \mathbb{F}_p[x]$ an irreducible monic polynomial of degree d, $f \mid x^{p^n} - x$ if and only if $d \mid n$. Furthermore $x^{p^n} - x$ is not divisible by the square of any irreducible polynomial.

So we suppose d satisfies $1 \leqslant d \leqslant n$ and $f \in \mathbb{F}_p[x]$ is an irreducible monic polynomial of degree d. Then we have $E = \mathbb{F}_p[x]/\langle f \rangle$ is a field with p^d elements, and $\alpha = [x] \in E$ satisfies $\alpha^{p^d} = \alpha$ (because E^* is a cyclic group of order $p^d - 1$). Now if $d \mid n$, then raising both sides of $\alpha^{p^d} = \alpha$ to the p^d power q times, where $n = qd$, gives us that $\alpha^{p^n} = \alpha$ in E. And this means that $\alpha^{p^n} - \alpha = [x^{p^n} - x] = [0] \in E = \mathbb{F}_p[x]/\langle f \rangle$, in other words, $x^{p^n} - x \in \langle f \rangle$, in other words $f \mid x^{p^n} - x$.

Now let's assume that the monic irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree d divides $x^{p^n} - x$ and we wish to show that $d \mid n$. Once again consider the field $E = \mathbb{F}_p[x]/\langle f \rangle$, and let $g(x) = x^{p^n} - x \in E[x]$. Clearly $1 \in E$ satisfies $g(1) = 0$, and $\alpha = [x] \in E$ satisfies $g(\alpha) = 0$, since $f \mid g$ and $f(\alpha) = 0$ in E. Now use the "freshman's dream" to conclude that the set of elements e of E which satisfy $g(e) = 0$ is a subring of E, and hence it is all of E. But E has p^d elements, so E^* is a cyclic group of order $p^d - 1$. And if σ is a generator of E^* then $\sigma^{p^d - 1} = 1$, and also $\sigma^{p^n - 1} = 1$ since this is true for all elements of E^*. Thus $p^d - 1 \mid p^n - 1$. We claim that this implies $d \mid n$ and will prove this below.

Up to this point, we've shown that the $x^{p^n} - x$ is the product of the monic irreducible polynomials of degrees d which divide n. Now we have to show that none of these irreducible polynomials occur to a power higher than 1 in the factorization of $x^{p^n} - x$. But if f is an irreducible factor of $x^{p^n} - x$, then f^2 cannot divide evenly into $x^{p^n} - x$, since the derivative of $x^{p^n} - x = p^n x^{p^n - 1} - 1 = -1$ in $\mathbb{F}_p[x]$ (and use the first sentence on page 3).

So the last detail we have to take care of is a proof that if t, d and n are positive integers, with $t > 1$, then $t^d - 1 \mid t^n - 1$ if and only if $d \mid n$. Start by writing $n = dq + r$ with $0 \leqslant r < d$. Then

$$\begin{aligned}\frac{t^n - 1}{t^d - 1} &= \frac{(t^d)^q t^r - 1}{t^d - 1} = \frac{(t^d)^q t^r - t^r + t^r - 1}{t^d - 1} \\ &= t^r \frac{(t^d)^q - 1}{t^d - 1} + \frac{t^r - 1}{t^d - 1} \\ &= t^r (1 + t^d + \cdots + (t^d)^{q-1}) + \frac{t^r - 1}{t^d - 1}\end{aligned}$$

But $0 \leqslant t^r - 1 < t^d - 1$, so the division works if and only if $r = 0$. This completes the proof of the theorem.

If we take the degree of both sides of the factorization $x^{p^n} - x = f_1 \cdots f_k$ from the theorem, we get the equation

$$p^n = \sum_{d \mid n} d N_d$$

where N_d is the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[x]$.

Since we know that there are p monic irreducible polynomials of degree 1 in $\mathbb{F}_p[x]$, namely

$$x, \quad x - 1, \quad x - 2, \quad \ldots, \quad x - (p - 1)$$

we have $N_1 = p$. So if q is a prime number, then

$$p^q = q N_q + N_1 = q N_q + p$$

and we can conclude that

$$N_q = (p^q - p)/q.$$

More generally, we have

$$N_n = \frac{1}{n} \left(p^n - \sum_{d < n, d \mid n} d N_d \right).$$

Another important consequence of the theorem above is the following lemma:

Lemma: Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree d. Then $f \mid x^{p^d} - x$ and f does not divide $x^{p^c} - x$ if $c < d$.

Using this result we can find factors of a given polynomial $f \in \mathbb{F}_p[x]$ using the Euclidean algorithm. Suppose that $g \in \mathbb{F}_p[x]$, $\deg(g) = d$ and $g = g_1 g_2 \cdots g_d$ where g_i is the product of all the irreducible polynomials of degree i that divide g. It then follows from the theorem that $\gcd(x^{p^i} - x, g)$ is the product of all the g_j for $j \mid i$. So we can find the g_j by successively inserting $i = 1, 2, \ldots$ into $\gcd(x^{p^i} - x, g)$ and using the Euiclidean algorithm to compute the gcd.

Factoring in $\mathbb{F}_p[x]$: We can use linear algebra to help decide whether a polynomial in $\mathbb{F}_p[x]$ of degree $\geqslant 4$ is irreducible. To do this, we consider the Frobenius map $F\colon \mathbb{F}_p \to \mathbb{F}_p$ where $F(\lambda) = \lambda^p$

(this is a ring homomorphism because of the "freshman's dream"). Given a polynomial $f \in \mathbb{F}_p[x]$ we extend F to the ring $R = \mathbb{F}_p[x]/\langle f \rangle$, and we'll still call this map $F\colon R \to R$.

But we can view R as a vector space over $\mathbb{F}_p$, and because $\lambda^p = \lambda$ for $\lambda \in \mathbb{F}_p$, the map F (extended to R) is a linear mapping of vector spaces. It might help to do an example of this.

Example: Let $f = x^5 + x + 1 \in \mathbb{F}_2[x]$. Then $R = \mathbb{F}_2[x]/\langle f \rangle$ is a vector space over $\mathbb{F}_2$ with basis $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ where $\alpha = [x]$. Since $f(\alpha) = 0$ in R, we have that $\alpha^5 = \alpha + 1$. What doe the Frobenius map $F(\lambda) = \lambda^2$ do to this basis? Well, $F(1) = 1$, $F(\alpha) = \alpha^2$, $F(\alpha^2) = \alpha^4$, $F(\alpha^3) = \alpha^6 = \alpha(\alpha^5) = \alpha(\alpha+1) = \alpha^2 + \alpha$, and $F(\alpha^4) = \alpha^8 = \alpha^3(\alpha^5) = \alpha^3(\alpha+1) = \alpha^4 + \alpha^3$. Therefore the matrix of the map F with respect to this basis is

$$M_F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Note that this matrix is invertible, since if we apply the permutation (2453) to it, it becomes upper triangular with 1s on the diagonal (so $\det M_F = 1$).

Now if M_F were *not* invertible, then we could find a non-constant polynomial $g \in \mathbb{F}_p[x]$ such that $\deg(g) < \deg(f)$ and $[g]^p = 0$. And if q were an irreducible polynomial such that $q \mid f$ then we would have $q \mid g$. Therefore $\gcd(f, g)$ is a non-trivial divisor of f (i.e., $0 < \deg(\gcd(f, g)) < \deg(f)$).

Next, suppose $g \in \mathbb{F}_p[x]$ is a polynomial such that $0 < \deg(g) < \deg(f)$ and $[g]^p - [g] = 0$ in $R = \mathbb{F}_p/\langle f \rangle$. In other words, $[g]$ is in the kernel of the linear map $F - I\colon R \to R$ (viewing R as a vector space over $\mathbb{F}_p$). Since

$$x^p - x = x(x-1)\cdots(x-p+1)$$

in $\mathbb{F}_p[x]$, we also have the factorization

$$g^p - g = g(g-1)\cdots(g-p+1)$$

in $\mathbb{F}_p[x]$. If q is an irreducible factor of f, and since $f \mid g^p - g$ (because $[g^p - g] = 0 \in R = \mathbb{F}_p/\langle f \rangle$), we obtain that q will divide one of g, $g-1$,…,$g-p+1$. And so one of $\gcd(f, g)$, $\gcd(f, g-1)$,…,$\gcd(f, g-p+1)$ is a non-trivial factor of f (since $\deg(g) < \deg(f)$).

Example (continued): The matrix of $F - I$ for the example above is

$$M_{F-I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Now $[1,0,0,0,0]^T \in \ker(M_{F-I})$, but we knew that would happen since $a^p - a = 0$ for all $a \in \mathbb{F}_p$. But there is a second, linearly independent element of $\ker(M_{F-I})$, namely $[1,1,0,1,1]^T$. This means that the polynomial $g = 1 + x + x^3 + x^4$ satisfies $f \mid g^2 - g$. Using the Euclidean algorithm, we can compute that

$$\gcd(x^5 + x + 1, x^4 + x^3 + x + 1) = x^2 + x + 1$$

and so $x^2 + x + 1$ is a nontrivial factor of $x^5 + x + 1$.

So we have a way to find non-trivial factors of polynomials in $\mathbb{F}_p[x]$. It might be a bit surprising to know that if the method given above doesn't work to find a factor of f, then f is irreducible:

Theorem: Suppose $f \in \mathbb{F}_p[x]$ is a non-constant polynomial and let $F\colon R \to R$ be the Frobenius map, where $R = \mathbb{F}_p[x]/\langle f \rangle$. Then f is irreducible if and only if $\ker(F) = 0$ and $\ker(F - I) = \mathbb{F}_p$.

Proof. We have seen above that $\ker(F) = 0$ and $\ker(F - I) = \mathbb{F}_p$ if f is irreducible, since otherwise we can use the method above to find a non-trivial factor of f. So conversely, assume that $\ker(F) = 0$ and $\ker(F - I) = \mathbb{F}_p$, and let r be a non-zero element of R. We're going to show that r is invertible in R, which will imply that R is a field, and thus that f is irreducible. Consider the $\mathbb{F}_p$-linear map $A\colon R \to R$ given by $A(x) = rx$, and suppose that $x \in \ker(A) \cap \operatorname{im}(A)$. Then $x = ry$ for some $y \in R$ and $rx = 0$. But then $F(x) = F(ry) = r^p y^p = r^{p-2} y^{p-1} rx = 0$, and so $x \in \ker(F)$. Therefore $x = 0$ and so $\ker(A) \cap \operatorname{im}(A) = 0$. But since $\dim(\ker(A)) + \dim(\operatorname{im}(A)) = \dim(R)$ (the dimensions are taken as vector spaces over $\mathbb{F}_p$), we have $\ker(A) + \operatorname{im}(A) = R$

Now, if $x \in \ker(A)$ then so is $F(x)$, since $A(F(x)) = rx^p = (rx)x^{p-1} = 0$. Likewise, if $x \in \operatorname{im}(A)$ then so is $F(x)$, since if $x = A(y) = ry$ then $F(x) = x^p = (ry)^p = r(r^{p-1}y^p) \in \operatorname{im}(A)$. We can express $1 \in R$ uniquely as $x + y$ where $x \in \ker(A)$ and $y \in \operatorname{im}(A)$. But then $F(1) = 1 = F(x) + F(y)$, and so $F(x) = x$ and $F(y) = y$. But since $\ker(F - I) = \mathbb{F}_p$ we have $x \in \mathbb{F}_p$ and $y \in \mathbb{F}_p$. The only way x can also be in $\ker(A)$ is for $x = 0$ (since x is a "scalar"), and so $y = 1$. But now $1 \in \operatorname{im} A$ so there is a $z \in R$ such that $rz = A(z) = 1$, and we are done.