Number Theory

May 14, 2008

Number Theory is the study of the mysterious and hidden properties of $\mathbb{Z}$ and $\mathbb{Q}$; it is the oldest part of mathematics. To this day it is quite an experiment-based field; we spot things which are happening by experiment, and then the hard pard is proof; even today many great conjectures remain unproven, and when they are proven this is usually as a result of great advances in seemingly distant areas.

The great modern development in number theory has been the rise of computer science; computer methods make numerical experiments much easier, and conversely computer science is fundamentally dependent on number theory.

There is one particularly recommended book for this course, Bomerance and Grandall's Primes - A Computational Approach.

1 Revision

1.1 Euclid's Algorithm

Given integers $a > 0, b$ we can find $q, r \in \mathbb{Z}$ such that $b = aq + r$ with $0 \leq r < a$: consider $\{b - xa : x \in \mathbb{Z}\}$; this set clearly contains elements ≥ 0 so it contains a least element ≥ 0; call this $r = b - qa$; then $r < a$ as were $r \geq a$ then $r - a \geq 0$ contradicting the definition of r.

A consequence of this is the existence of the gcd of any two integers a, b not both zero; given such a, b define $I = \{xa + yb : x, y \in \mathbb{Z}\}$

1.1.1 Lemma

$\exists d > 0 \in \mathbb{Z}$ such that $I = d\mathbb{Z}$: I contains elements > 0, take d to be the least such element, then for any $c \in I$ we can write $c = qd + r$ where $0 \leq r < d$; then we have $r \in I$ so $r = 0$ and we are done.

Note that $d \mid a, d \mid b$, and if $e \mid a, e \mid b$ then $e \mid$ every element of I; in particular, $e \mid d$; hence d is the gcd of a and b, written (a, b). This argument shows that every ideal in $\mathbb{Z}$ is principal; note that this is false in a general ring e.g. $R = \{x + y\sqrt{m} : x, y \in \mathbb{Z}\}$.

Now, given a, b both positive with $a < b$, Euclid's algorithm gives us a very efficient way of computing $d = (a, b)$: we write $b = aq_1 + r_1, a = r_1q_2 + r_2, r_! = r_2q_3 + r_3$ etc. with $r_1 < a, r_2 < r_1$ etc. until $r_{n-1} = r_nq_{n+1}$; this process must terminate as the r_i are a decreasing sequence of positive integers. Observe that

$r_n = (r_n - 1, r_n) = \cdots = (r_1, r_2) = (a, r_1) = (a, b)$. A fundamental consequence of this, which bizzarely is never stated in Euclid, is:

1.2 Unique Prime Factorization

We define that an integer $n > 1$ is prime if n has no nontrivial factorization; i.e. if $n = ab$ for $a, b \in \mathbb{N}$ then $\{a, b\} = \{1, n\}$.

1.2.1 Lemma

Let p be any prime number, then if $p \mid ab$ then $p \mid a$ or $p \mid b$; assume $p \nmid a$, then $(a, p) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ such that $ax + py = 1 \therefore abx + pby = b$; then $p \mid$ the left hand side since $p \mid ab$ so $p \mid$ the right hand side, i.e. b.

1.2.2 Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be written as a product of primes, and this representation is unique up to order: $n = n_1 n_2$ where $0 < n_1, n_2 < n$; by induction we have existence. For uniqueness suppose $p_1 \dots p_r == q_1 \dots q_j$, then $p_1 \mid q_1 \dots q_j \therefore$ either $p_1 = q_1$ or $p_1 \mid q_2 \dots q_j$, etc.

An algorithm is called <u>polynomial</u> if when applied to M it takes $\leq c(\log M)^W$ elementary operations, where c, W are positive constants. For example, if M, R have m, r digits respectively, computing MR can be done in at most $2mr$ elementary operations, and we clearly have $m \leq \log M + 1$ etc. so if $R \leq M$ then the maximum number of operations required to multiply R and M is $\leq 2(\log M + 1)^2$ - we have a polynomial algorithm for multiplication. The obvious algorithm for factoring an integer $N > 1$ (or telling us it is prime) is trial division by 2 and all odd integers $\leq \sqrt{n}$, but this is not polynomial; a fundamental question is whether a polynomial algorithm for factoring exists (note that there are polynomial algorithms for primality testing, but these only tell us whether N is prime, they do not find a factor of it).

The largest known prime is currently $2^{32582657} - 1$.

1.2.3 Theorem (Euclid)

There are infinitely many primes: let $2, 3, \dots, p$ be the primes $\leq p$, then $N = 2 \times 3 \times \cdots \times p + 1$ must have a prime factor $> p$.

1.2.4 Theorem

Let N be any integer ≥ 2, then $\exists$ blocks of consecutive <u>composite</u> numbers whose length is $\geq N$: pick $p \geq N + 2$ prime, then consider the $p - 1$ numbers $M + 2, M + 3, \dots, M + p$ where $M = 2 \times 3 \times \cdots \times p$; each of these integers must be <u>composite</u> since they are divisible by a prime $\leq p$ but $> p$.

1.2.5 Three unproven statements thought to be true

There are infinitely many twin primes.

There are infinitely many triple primes of the form $(p, p + 2, p + 6)$ (or $(p, p + 4, p + 6)$; note if we have $(p, p + 2, p + 4)$ one of these is divisible by 3).

There are infinitely many primes of the form $n^2 + 1$.

1.2.6 Definition

For $x \geq 2$, $\pi(x)$ = the number of primes $\leq x$; we have $\pi(10^2) = 25, \pi(10^3) = 168, \pi(10^4) = 1229, \pi(10^6) = 78498$.

1.2.7 Guess of Gauss

$\pi(x)$ is close to $\mathrm{li}(x) := \int_2^x \frac{dt}{\log t}$; this is remarkably accurate, see later.

The above Euclid implies $\pi(x) > \log\log x$ for $x > 2$; we can do better than this. Let S be any finite set of prime numbers, and define $f_S(x)$ = the number of positive integers $\leq x$ which are composed of primes in S.

Lemma: $\forall x \geq 2, f_S(x) \leq \sqrt{x} \times 2^{\#(S)}$: if n is composed only of primes in S we can write $n = m^2 r$ where r is square-free; then $n \leq x \Rightarrow m^2 \leq x \Rightarrow m \leq \sqrt{x}$ so there are at most $\sqrt{x}$ possible choices of m, while r is of the form $p_1 \dots p_s$ where the p_i are distinct primes from S so the total number of choices of r is $\leq 2^{\#(S)}$.

Corollary: for $x \geq 2, \pi(x) \geq \frac{\log x}{2 \log 2}$ by letting S be the set of all primes $\leq x$, then $f_S(x) = x \leq \sqrt{x} 2^{\pi(x)}$; rearranging gives the result.

We can do still better than this, even by elementary methods; see Chebyshev.

1.3 Congruences

Take an integer $m > 1$. We define $a \equiv b \mod m$ if $m \mid a - b$; this is an equivalence relation on $\mathbb{Z}$ with equivalence classes $a + m\mathbb{Z}$; we write $\mathbb{Z}/m\mathbb{Z}$ for the set of such equivalence classes. Addition and multiplication of classes is defined in the obvious way.

Lemma: $a + m\mathbb{Z}$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ iff $(a, m) = 1$: $(a + m\mathbb{Z})(b + m\mathbb{Z}) = 1 + m\mathbb{Z}$ for some b iff $ab + mk = 1$ for some b and k, iff $(a, m) = 1$ by Euclid's algorithm.

We define $(\mathbb{Z}/m\mathbb{Z})^\star$ to be the group of units of $\mathbb{Z}/m\mathbb{Z}$ and Euler's function $\phi(m) = \#((\mathbb{Z}/m\mathbb{Z})^\star)$.

1.3.1 Euler's Theorem

If a is an integer prime to m then $a^{\phi(m)} \equiv 1 \mod m$: this is true by Lagrange's theorem since $\phi(m)$ is the order of the group of units modulo m so the order of a must divide it. If $m = p$ prime then $\phi(m) = p - 1$ so we have:

1.3.2 Corollary: Fermat's Little Theorem

If $(a, p) = 1$ then $a^{p-1} \equiv 1 \mod p$. Therefore for p an odd prime, $2^{p-1} \equiv 1 \mod p$.

When do we have $2^{p-1} \equiv 1 \mod p^2$? There are only two known such examples, 1093 and 3511, and these are known to be the only such $p < 16 \times 10^{12}$, but it is unknown whether this is the case for infinitely many primes, or even whether there are infinitely many primes for which $2^{p-1} \not\equiv 1 \mod p^2$.

1.3.3 Chinese Remainder Theorem

For $k \geq 1$ and $m_1, \ldots, m_k$ distinct with $(m_i, m_j) = 1 \forall i \neq j$, put $M = m_1, \ldots m_k$. Given any integers $a_1 \ldots a_k$, $\exists x \in \mathbb{Z}$ with $x \equiv a_1 \mod m_1, \ldots, x \equiv a_k \mod m_K$; moreover any two such m are congruent modulo M. This last part is obvious; if x, y are two solutions then $m_i \mid x - y \forall i \therefore M \mid x - y$, and for the existence of such n x put $M_i = \frac{M}{m_i}$, then $(M_i, m_i) = 1$ so $\exists u_i : u_i M_i \equiv 1 \mod m_i$, then take $x = \sum_{i=1}^{k} a_i u_i M_i$.

We can take a more abstract approach to the CRT: let $R_i = \frac{\mathbb{Z}}{m_i \mathbb{Z}}$, then define the cartesian product $R_1 \times \cdots \times R_k = \{(x_1, \ldots, x_k) : x_i \in R_i\}$ by componentwise addition and multiplication. Then $R_1 \times \cdots \times R_k$ is a ring and we can reformulate the CRT as the following:

Theorem: Assume $(m_i, m_j) = 1 \forall i \neq j$, let $M = m_1 \ldots m_k$. Then the map $\theta : \frac{\mathbb{Z}}{M\mathbb{Z}} \to R_1 \times \cdots \times R_k$ defined by $\theta(a + M\mathbb{Z}) = (a + m_1\mathbb{Z}, \ldots, a + m_k\mathbb{Z})$ is an isomorphism of rings: the map is well defined and preserves addition and multiplication; it is injective since $\theta(a+M\mathbb{Z}) = \theta(b+\mathbb{Z}) \Rightarrow m_i \mid a-b \forall i \Rightarrow M \mid a-b$. Then surjectivity is automatic as $\#(\frac{\mathbb{Z}}{M\mathbb{Z}}) = m = \#(R_1 \times \cdots \times R_k)$; in practice this proof is less useful than the previous one as it is nonconstructive.

Corollary: If $(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$ as $\phi(r) = \#((\frac{\mathbb{Z}}{r\mathbb{Z}})^\star)$ and θ induces an isomorphism $(\frac{\mathbb{Z}}{mn\mathbb{Z}})^\star \to (\frac{\mathbb{Z}}{m\mathbb{Z}})^\star \times (\frac{\mathbb{Z}}{n\mathbb{Z}})^\star$.

1.4 Solution of congruences of the form $f(X) \equiv 0 \mod m$ where $f(X) \in \mathbb{Z}[X]$

As a surprising example $f(X) = X^2 - 1$ has four roots mod 8 (1,3,5,7); thus we do not have a fundamental theorem of algebra like in $\mathbb{C}$ where a polynomial of degree n has at most n roots.

Let R be a ring; define $R[X]$ is the set of formal expressions $a_0 + \cdots + a_n X^n$ for $a_i \in R$; add and multiply polynomials in the usual way. Then for $f(X) \in R[X], \alpha \in R$ we define $f(\alpha) = a_0 + \cdots + a_n \alpha^n \in R$.

Lemma: For $f(X) \in R[X], \alpha \in R \exists h(X) \in R[x]$ such that $f(X) - f(\alpha) = (X - \alpha)h(X)$: $f(X) = a_0 + \cdots + a_n X^n \therefore f(X) - f(\alpha) = a_1(X - \alpha) + \cdots + a_n(X^n - \alpha^n)$, but $X^k + \alpha^k = (X - \alpha)(X^{k-1} + x^{k-2}\alpha + \cdots + \alpha^{k-1})$ (and this is true in any ring).

Corollary: $f(\alpha) = 0 \Leftrightarrow \exists h(X) \in R(X) : f(x) = (X - \alpha)h(X)$.

Definition: $\alpha \neq 0 \in R$ is a <u>zero divisior</u> if $\exists \beta \neq 0 \in R$ with $\alpha\beta = 0$, e.g. $2 + 8\mathbb{Z}$ in $\frac{\mathbb{Z}}{8\mathbb{Z}}$.

Definition: the ring R is an <u>integral domain</u> if R has no zero divisors; examples are $\mathbb{Z}$ and any field such as $\frac{\mathbb{Z}}{p\mathbb{Z}}$. If $f(X) = a_0 + \cdots + a_n X^n$ we define $\deg f = n$; $\deg 0 = -\infty$

Lemma: if R is an integral domain then $\deg fg = \deg f + \deg g$; let $f(X) = a_n X^n + \cdots + a_0 \neq 0 \neq g(X) = b_m X^m + \cdots + b_0$ (the result trivially holds if f or g is 0), then $fg(X) = a_n b_m X^{m+n} + \ldots$ with $a_n b_m \neq 0$.

Proposition: let R be an ID and $\alpha_1, \ldots, \alpha_s \in R$ distinct roots of $f(X) \not\equiv 0 \in R[X]$, then $\exists g(X) \in R[X]$ such that $f(X) = (X - \alpha_1) \ldots (X - \alpha_s) g(X)$; in particular $s \leq \deg f$. We have already proven this for $s = 1$, then induction; assuming this is true for s, take α_{s+1} distinct from $\alpha_1, \ldots, \alpha_s$ with $0 = f(\alpha_{s+1}) = (\alpha_{s+1} - \alpha_1) \ldots (\alpha_{s+1} - \alpha_s) g(\alpha_{s+1})$; $\alpha_{s+1} - \alpha_i \neq 0 \forall i$, so since R is an ID the probuct $(\alpha_{s+1} - \alpha_1) \ldots (\alpha_{s+1} - \alpha_s) \neq 0$ and so $g(\alpha_{s+1}) = 0 \therefore g(X) = (X - \alpha_{s+1})h(X)$ as required.

Corollary: Lagrange's theorem: let p be a prime and $a_0, \dots, a_n$ integers with $a_n \not\equiv 0 \mod p$; then the congruence $a_nX^n + \cdots + a_0 \equiv 0 \mod p$ has at most n (incongruent) solutions mod p; take $R = \frac{\mathbb{Z}}{p\mathbb{Z}}, f(X) = \overline{a_n}X^n + \cdots + \overline{a_0}$ where $\overline{a_i} = a_i + p\mathbb{Z}$; $f \not\equiv 0$ since $\overline{a_n} \neq 0$ so there are at most n solutions in $\frac{\mathbb{Z}}{p\mathbb{Z}}$ by the above.

For example, $f(X) = X^{p-1} - 1 - (X-1) \times \cdots \times (X-(p-1))$; has $\deg f < p-1$ but by Fermat's little theorem it has $p-1$ roots modulo p, so $f \equiv 0$ (i.e. each of its coefficients is 0 modulo p) by Lagrange's Theorem.

Corollary: Wilson's Theorem: for p prime, $(p-1)! \equiv -1 \mod p$; note that conversely if $n > 1$ is an integer, then $(n-1)! \equiv -1 \mod n \Rightarrow n$ is a prime (but this cannot be used for an efficient primality test). When do we have $(p-1)! \equiv -1 \mod p^2$? The known examples are $p = 5, 13, 8563$ and these are the only such primes $< 5 \times 10^8$, but as usual we don't know whether there are infinitely many such p.

1.5 Theorem of the Primitive Root

Theorem: If F isa field of finite cardinality (i.e. with finitely many elements) then $F^\times$ is cyclic, e.g. F_p [I will write F_p for $\frac{\mathbb{Z}}{p\mathbb{Z}}$ and a for $a + p\mathbb{Z}$]. Any generator of $F_p^\times$ is called a primitive root $\mod p$, e.g. $2 \mod 11$.

Artim's (unproven) conjecture: $n = 2$ is a primitive root for infinitely many primes p (in fact, Artim's conjecture is that this is the case for any $n \neq \pm 1$ which is not a square).

Remark: if G is any cyclic group of order d then G has precisely $\phi(d)$ elements of (exact) order d; let $G = \langle g \rangle$ (i.e. the group generated by g), then g^i generates $G \Leftrightarrow (i, d) = 1$.

Lemma: let $n \geq 1$ be an integer, then $n = \sum_{d|n, d\geq 1} \phi(d)$: for each $d \geq 1$ with $d \mid n$ let C_d be the unique subgroup of F_n of order d; let Φ_d be the set of generators such that $|\Phi_d| = \phi(d)$. Then, and this is the key remark, $C_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$ is the disjoint union of the Φ_d as d runs over all divisors of $n \geq 1$, so $n = \#(C_n) = \sum_{d|d, d\leq n} \#(\Phi_d)$ and we have the result.

Proposition: Let H be any finite group of order n. Suppose that for all $d \mid n$, $|\{x \in H : x^d = 1\}| \leq d$, then $H \cong C_n$: For each $d \mid n$ let W_d be the set of $x \in H$: with exact order d. For $W_d \neq \emptyset$ take $y \in W_d$, then $\langle y \rangle = \{1, y, \dots, y^{d-1}\}$ has d elements, and $x^d = 1 \forall d \in \langle y \rangle$ so $W_d = \langle y \rangle$. And H has precisely $\phi(d)$ elements of exact order d so $\#(W_d) = \phi(d)$. Or if $W_d = \emptyset$ for some $d \mid n$, this is impossible since $n = \#(H) = \sum_{d|n} \phi(d)$ so we would have $\#(H) < n$, a contradiction. Taking $d = n$,H must be cyclic since $W_n \neq \emptyset$.

Corollary: If F is a finite field then $F^\times$ is cyclic: $X^d - 1 \in F[X]$ has at most d roots and they are $\in F^\times$ so $H = F^\times$ must be cyclic.

For p prime, consider the ring $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$; this is not a field for $n > 1$ as then p is a zero divisor.

Herafter p is an odd prime.

Theorem: $\forall n \geq 1$, $(\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ is cyclic.

Proposition: $\exists$ a primitive root $g \mod p$ such that $g^{p-1} = 1 + bp$ with $(b, p) = 1$, and any such g generates $(\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times \forall n \geq 1$, e.g. 3 for $p = 7$: for the first part take any primitive root g_1, and consider $g_1^{p-1} = 1 + b_1p$; if $(b_1, p) = 1$ we are done, otherwise $p \mid b_1$; then set $g = g_1 + p$ and this is a primitive root mod p but $g^{p-1} = 1 + bp$ with $(b, p) = 1$ since $g^{p-1} - 1 = (g_1 + p)^{p-1} - 1 = g_1^{p-1} - 1 + (p-1)g_1^{p-2}p + p^2a$ for some $a \in \mathbb{Z}$, i.e. $(p-1)g_1^{p-2}p + p^2c$ for $c \in \mathbb{Z}$, but this is $((p-1)g_1^{p-2} + pc)p = bp$ with $p \nmid b$. For the second part we will use the following:

Lemma: Let $w = 1 + pb$ where $(p, b) = 1$, then $\forall n \geq 0$, $wp^n = 1 + b_n p^{n+1}$ with $(b_n, p) = 1$: induction, the $n = 0$ case is true by hypothesis, now assuming it's true for n then $w^{p^{n+1}} = (1 + b_n p^{n+1})^p \therefore w^{p^{n+1}} - 1 = b_n p^{n+2} + \sum_{i=2}^{p} \binom{p}{i} b_n^i p^{(n+1)i} = b_n p^{n+2} + \frac{p(p-1)}{2} b_n^2 p^{2n+2} + p^{2n+3} c_n$ for some $c_n \in \mathbb{Z}$, but since p is odd, $p \mid \frac{p(p-1)}{2}$ so this is $b_n p^{n+2} + a_n p^{2n+3}$ for some $a_n \in \mathbb{Z}$, $= p^{n+2}(b_n + pa_n)$; let the bracket be b_{n+1} and then $p \nmid p_{n+1}$ since $p \nmid b_n$.

Now to complete the proof we induct on n; the $n = 1$ case is by hypothesis; $w = g^{p-1}$ must have order p in $(\frac{\mathbb{Z}}{p^2\mathbb{Z}})^\times$, and we continue by induction.

2 Law of Quadratic Reciprocity

This was discovered by Legendre in c. 1785, but not proven until Gauss in 1796; this is the form we shall proove (using a proof given by Gauss). In the 19th century a major theme was to generalize this to cubic, quartic, etc. reciprocity; in 1927 E. Artim proved the general abelian reciprocity law. Non-abelian reciprocity has been studied since 1965 and remains an important research topic today.

Lemma: In $F_p^\times$ there are precisely $\frac{p-1}{2}$ squares: $F_p^\times = \{1, g, \ldots, g^{p-2}\}$ for some primitive root g; g^i is a square $\Leftrightarrow$ i is even; the forward implication is trivial, for the converse if $g^i = y^2$ then let $y = g^k$, then $g^{2k} = g^2$ so $i \equiv 2k \mod p-1$ so since $p-1$ is even, $2 \mid i$.

Definition: let a be any integer with $(a, p) = 1$; we say a is a quadratic nonresidue if it is a square in F_p and a quadratic non-residue otherwise; we define the legendre symbol $(\frac{a}{p})$ to be 0 if $p \mid a$, 1 for a a quadratic residue mod p and -1 for a a quadratic non-residue mod p.

Lemma (Euler's Criterion): $\forall a \in \mathbb{Z}, (\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \mod p$; a corollary is that $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$, which shows that $a \mapsto (\frac{a}{p})$ defines a group homomorphism $F_p^\times \to \{\pm 1\}$. Putting $a = 1$ we have $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, i.e. -1 is a square modulo $p \Leftrightarrow p \equiv 1 \mod 4$. For the proof of the lemma let $P = \frac{p-1}{2}$; if $p \mid a$ the result is trivial as both sides are $0 \mod p$, otherwise we have $a^{p-1} \equiv 0 \mod p$ by FLT so since the LHS is $(a^P - 1)(a^P + 1)$ we have eithr $a^P \equiv 1 \mod p$ or $a^P \equiv -1 \mod p$, but these cannot simultaneously be true. Let g be a generator of F_p, then $a \equiv g^k \mod p$ for some $k \in \mathbb{Z}$ so $a^P = g^{kp} \mod p$; if we assume k even, i.e. a is a quadratic residue modulo p, i.e. $(\frac{a}{p}) = +1$, then $kP = k\frac{p-1}{2}$ is an integer multiple of $p-1$, so $g^{kP} \equiv 1 \mod p$ and we have the result; otherwise k is odd i.e. $(\frac{a}{p}) = -1$, then kP is not an integer multiple of $p-1$, so $g^{kP} \neq 1 \mod p$; since g is a primitive root $\mod p$ this implies $a^P \not\equiv 1 \mod p$; by the earlier remark $a^P \equiv -1 \mod p$ as required.

2.1 Theorem (Law of Quadratic Reciprocity

Let p, q distinct odd primes, then $(\frac{p}{q}) = (\frac{q}{p})$ iff at least one of p and q is $1 \mod 4$; equivalently $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. This is perhaps the first nonobvious proof in this course; we shall proove it in the next lecture.

Lemma of Gauss: Let a be an integer with $(a, p) = 1$; define P as before. For $j = 1, \ldots, P$ let a_j denote the unique integer with $a_j = ja \mod p$ and $-\frac{p}{2} < a_j < \frac{p}{2}$, i.e. $a_j \in \{\pm 1, \pm 2, \ldots, \pm P\}$. Le $\nu(a)$ denote the number of j for which $a_j <$ [; then $(\frac{a}{p}) = (-1)^{\nu(a)}$: if $j_1 a = j_2 a \mod p$ then $p \mid j(a_1 - a_2)$ so $j_1 = j_2$; if $j_1 a = -j_2 a \mod p$ then $p \mid (j_1 + j_2)a \Rightarrow p \mid j_1 + j_2$ which is impossible, so the P elements a_j as j runs from 1 to P consist of precisely $\{epsilon_1 1, \epsilon_2 2, \ldots, \epsilon_P P\}$ where $\epsilon_i = 1$ or -1. Hence $a \times 2a \times \cdots \times Pa = 1 \times 2 \times \dot{\times} P(-1)^{\nu(a)} \mod P \Rightarrow a^P \equiv (-1)^{\nu(a)} \mod P$, but by the previous lemma this is $\equiv (\frac{a}{p})$; both these are ± 1 and congruent $\mod p$, so $(\frac{a}{p}) = (-1)^{\nu(a)}$.

[After this lecture I dropped this course]