Finite Fields

(AKA Galois Fields)

November 24, 2008

The Field of p Elements (Review)

- By considering congruence mod n for any positive integers n we constructed the ring $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ of residue classes mod n.
- In $\mathbb{Z}_n$ we add, subtract, and multiply as usual in $\mathbb{Z}$, with the understanding that all multiples of n are declared to be zero in $\mathbb{Z}_n$.
- Algebraists often write $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ to emphasize the point that $n\mathbb{Z}$, the set of all multiples of n, is zero in the quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. (Technically, $n\mathbb{Z}$ is an *ideal* in the ring $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring by that ideal.)
- Using the Euclidean algorithm (which is based on the division algorithm) one shows that a residue class $a \in \mathbb{Z}_n$ is invertible if and only if $\gcd(a, n) = 1$.
- Hence, $\mathbb{Z}_n$ is a field[1] if and only if $n = p$ is a prime number.

[1] In a *field* every nonzero element is invertible.

The Field of p Elements (Review)

- Alternative notations for the field $\mathbb{Z}_p$ of p elements, when p is a prime, are: $\mathbb{F}_p$ or $GF(p)$ (GF stands for "Galois field.").
- Let's use the $\mathbb{F}_p$ notation for $\mathbb{Z}_p$ henceforth, to emphasize the fact that we are dealing with a field and not just a ring.

GENERALIZATION

- It turns out that there is a finite field $\mathbb{F}_q$ of $q = p^r$ elements, for every prime power p^r.
- Moreover, there are no other examples of finite fields.
- We will now discuss how to construct the finite fields F_q for $q = p^r$ where $r > 1$.

What is a ring, anyway?

A *ring* is a set R endowed with two operations called addition and multiplication, such that the following axioms hold for every $a, b, c \in R$:

- Addition is associative: $a + (b + c) = (a + b) + c$.
- Addition is commutative: $a + b = b + a$.
- Zero is neutral for addition: $a + 0 = a$.
- a has an opposite $-a$ (in R) such that $a + (-a) = 0$.
- Multiplication is associative: $a(bc) = (ab)c$.
- The element 1 is neutral for multiplication: $1a = a = a1$.
- Multiplication distributes across addition: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

A *commutative ring* is a ring which also satisfies the law: $ab = ba$ for all $a, b \in R$.

Fields, Ideals, and Quotient Rings

- By definition, a *field* is just a commutative ring in which every nonzero element has an inverse.
- An *ideal* in a ring R is a nonempty subset J of R satisfying:
  (a) $a - b \in J$ for all $a, b \in J$ (closure under subtraction);
  (b) ra and ar are in J, for all $a \in J$, $r \in R$ (closure under outside multiplication).
- Given an ideal J in a ring R, we define congruence mod J of two given elements $a, b \in R$ by declaring that $a \equiv b \pmod{J}$ whenever $a - b \in J$. This gives an equivalence relation on R. The resulting equivalence classes are the elements of the quotient ring R/J.
- For example, in $R = \mathbb{Z}$ the subset $n\mathbb{Z}$ is an ideal, and the resulting quotient ring is $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.
- THEOREM: If R is a commutative ring and J an ideal then R/J is a field if and only if J is a maximal ideal.

The polynomial ring $\mathbb{F}_p[x]$

- The polynomial ring $\mathbb{F}_p[x]$ is the set of all polynomials with coefficients from $\mathbb{F}_p$. These are expressions of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

  where each coefficient $a_i \in \mathbb{F}_p$. The set $\mathbb{F}_p[x]$ is an infinite set.
- Recall that the *degree* of a polynomial is the highest exponent of x which occurs in the polynomial. For instance, the polynomial $x^2 + x + 1$ has degree 2 and $4x + 1$ has degree 1.
- The degree of a constant polynomial is 0, except that by special agreement we define the degree of the zero polynomial to be -1 or sometimes $-\infty$.

The polynomial ring $\mathbb{F}_p[x]$

- In any given degree, there are only finitely many elements of $\mathbb{F}_p[x]$, since there are only a finite number of possibilites for each coefficient.
- We may add, subtract, and multiply polynomials in $\mathbb{F}_p$ as we learned in school. Even though the coefficients are elements of $\mathbb{F}_p$ instead of actual integers, it is easy to do the calculations so long as we remember to always reduce coefficients mod p.
- EXAMPLES. In $\mathbb{F}_5[x]$ we have:
  $(2x^2 + 4x + 1) + (4x^3 + 3x^2 + 4) = 4x^3 + 4x;$
  $(2x^2 + 4x + 1) - (4x^3 + 3x^2 + 4) = x^3 + 4x^2 + 4x + 2;$
  $(2x^2 + 4x + 1) \cdot (4x^3 + 3x^2 + 4) = 3x^5 + 2x^4 + x^3 + x^2 + x + 4.$
  Check these calculations for yourself.
- It is easy to check that $\mathbb{F}_p[x]$ is a commutative ring, for any prime p.

Division algorithm in $\mathbb{F}_p[x]$

- Of utmost importance is the fact that there is a division algorithm in $\mathbb{F}_p[x]$ by which one can divide any given polynomial $a(x)$ by another (nonzero) polynomial $b(x)$ and get a quotient polynomial $q(x)$ and a remainder polynomial $r(x)$:

$$a(x) = b(x)q(x) + r(x), \quad \deg r(x) < \deg b(x).$$

  The method is the familiar long division of polynomials from high-school algebra, except that one uses modular arithmetic on the coefficients.
- $q(x)$ is the *quotient polynomial* and $r(x)$ the *remainder polynomial*.
- EXAMPLE. Check that $4x^3 + 3x^2 + 4 = (3x^2 + 4x + 1)(3x + 2) + (4x + 2)$, by dividing $a(x) = 4x^3 + 3x^2 + 4$ by $b(x) = 3x^2 + 4x + 1$.

Euclidean Algorithm for $\mathbb{F}_p[x]$

- The Euclidean algorithm may be extended to $\mathbb{F}_p[x]$. It works just the same in $\mathbb{F}_p[x]$ as it does in $\mathbb{Z}$, except that one must replace ordinary long division of integers by long division of polynomials in $\mathbb{F}_p[x]$.
- The extended Euclidean algorithm also works: by working backwards with the equations coming from the Euclidean algorithm, one can always find polynomials $s(x)$ and $t(x)$ such that

$$\gcd(a(x), b(x)) = a(x)s(x) + b(x)t(x).$$

- Any commutative ring without zero divisors in which the Euclidean algorithm holds is called a *Euclidean domain*. The ring of polynomials with coefficients in a field is always a Euclidean domain.

Divisibility in $\mathbb{F}_p[x]$

- Let $a(x), b(x) \in \mathbb{F}_p[x]$. Say that $a(x)$ divides $b(x)$ (written as $a(x) \mid b(x)$) if there is a polynomial $q(x) \in \mathbb{F}_p[x]$ such that $b(x) = a(x)q(x)$.
- Every polynomial has lots of trivial factorizations. Since any nonzero $\alpha \in \mathbb{F}_p$ is invertible, we can always write $a(x) = \alpha \cdot \alpha^{-1} a(x)$ where $\alpha^{-1} a(x) \in \mathbb{F}_p[x]$. But note that in such a trivial factorization, the degree of the factors is 0 and $\deg a(x)$.
- We define a *nontrivial* factorization of $a(x)$ to be one of the form $a(x) = b(x)c(x)$ where the degrees of $b(x), c(x)$ are both strictly positive.
- **Definition:** A polynomial $a(x)$ is said to be *irreducible* in $\mathbb{F}_p[x]$ if it has no factorizations other than the trivial ones. For example, $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, as you should check.

Construction of the Finite Field $\mathbb{F}_q$

- Let $q = p^r$ with $r > 1$. To construct a field of q elements, choose an irreducible polynomial $p(x) \in \mathbb{F}_p[x]$, and define congruence in $\mathbb{F}_p[x]$ by declaring that $a(x) \equiv b(x) \pmod{p(x)}$ if and only if $a(x) - b(x)$ is a multiple of $p(x)$.
- Let $\mathbb{F}_q$ be the set of residues mod $p(x)$. This is just the set of all polynomials of degree strictly less than r. It is easy to see that there are precisely $q = p^r$ such polynomials.
- We define addition, subtraction, and multiplication in $\mathbb{F}_q$ by doing the operation first in $\mathbb{F}_p[x]$ and then reducing mod $p(x)$ if necessary.
- With these operations, it turns out that $\mathbb{F}_q$ is a field, as long as our starting polynomial $p(x)$ is irreducible. One can prove this using the extended Euclidean algorithm for polynomials, since it turns out that $a(x) \in \mathbb{F}_p(x)$ is invertible mod $p(x)$ if and only if $\gcd(a(x), p(x))$ divides 1.

Isomorphism Theorems

- The arithmetic in a given finite field depends on the choice of irreducible polynomial $p(x)$ used to construct it. Nevertheless, we do have the following results.
- **Theorem:** *$\mathbb{F}_q$ is isomorphic with the quotient ring $\mathbb{F}_p[x]/p(x)\mathbb{F}_p[x]$ where we have divided $\mathbb{F}_p[x]$ by the ideal consisting of all multiples of $p(x)$.*
- **Theorem:** *Any two finite fields of the same number of elements must be isomorphic.*
- For those of you who know about field extensions, note that $\mathbb{F}_q$ is isomorphic with an extension $\mathbb{F}_p(\omega)$, where ω is a new "number" satisfying the equation $p(\omega) = 0$. For instance, to construct $\mathbb{F}_4$ we can use the irreducible polynomial $p(x) = x^2 + x + 1$, so the new element ω satisfies $\omega^2 + \omega + 1 = 0$. So to get $\mathbb{F}_4$ from $\mathbb{F}_2$ we can simply adjoin the new element ω to $\mathbb{F}_2$.

An Example

The field $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$ consists of the residues $0, 1, x, x + 1$. These residues add and multiply according to the following tables:

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

·	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

where we have used the relation $x^2 + x + 1 = 0$ repeatedly to reduce products and sums, and of course all coefficients are read mod 2.

- Write $\mathbb{F}_q^*$ for the set of nonzero elements of $\mathbb{F}_q$.
- A *primitive root* in $\mathbb{F}_q$ is an element g of F_q^* such that the powers of g generate every element of $\mathbb{F}_q^*$. To say it another way, every element of $\mathbb{F}_q^*$ can be expressed as some power of g. Equivalently, $g^e \neq 1$ for any $e < q - 1$.

theorem

Let $F = \mathbb{F}_q$ be a Galois field of $q = p^r$ elements where $r \geq 1$. Then its group of units $\mathbb{F}_q^*$ contains a primitive root g. There are in fact $\varphi(q-1)$ such primitive roots in $\mathbb{F}_q^*$.

- Those of you who know something about group theory will recognize that this theorem simply says that *the multiplicative group of a finite field is always a cyclic group*.

Example

We construct $\mathbb{F}_8$ as the residue ring $\mathbb{F}_2[x]/(x^3+x+1)$, so in $\mathbb{F}_8$ we have the relation $x^3+x+1=0$, which is the same as $x^3=x+1$. Taking $g=x$, computing the powers and tabulating the results gives the table

e	1	2	3	4	5	6	7
g^e	x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1

Given an entry g^e in the bottom row, its exponent e in the top row is called the *index* or *logarithm* of g^e. Thus for instance $\log(x^2+x+1)=\text{index}(x^2+x+1)=5$. These indices are known as discrete logarithms.

Note that once we know the table of indices, it is simple to multiply any two elements, by simply adding their indices ($\log AB=\log A+\log B$). Thus from the above table of indices we read off that $(x^2+x+1)\cdot(x^2+1)=x^2+x$ since $5+6=4 \mod 7$. (We add exponents modulo $7=q-1$ because $g^7=1$.)

Applications to Cryptography

- Fix a primitive root g for $\mathbb{F}_q^*$, where q is large.
- Using successive squaring, it is possible to quickly (in polynomial time) compute $Y = g^X$ for any positive integer X. (We only care about $1 \leq X \leq q - 1$.)
- It is believed that given some polynomial $Y \in \mathbb{F}_q^*$ it is computationally impractical to compute the logarithm X, for q sufficiently large.
- In other words, it is generally believed that the function $f(X) = g^X$ is a one-way function.
- However, no proof of this belief yet exists.

Diffie-Hellman Key Exchange

- How can two users agree on a secret key (used perhaps for a classical cryptosystem) over a public channel?
- The users agree on a large prime power $q = p^r$ and a primitive root $g \in \mathbb{F}_q$. Both g and q are public.
- User A randomly chooses an integer a between 1 and $q - 1$ and user B randomly chooses an integer b in the same range. The integers a, b are kept secret.
- User A computes the residue $g^a \in \mathbb{F}_q$, and user B computes $g^b \in \mathbb{F}_q$. Each user sends their computed power residue to the other.
- Both users can easily compute $g^{ab} \in \mathbb{F}_q$, simply by raising the element they receive to their secret exponent, since $g^{ab} = (g^a)^b = (g^b)^a$. This computed element g^{ab} is the secret key they have agreed upon.
- It is known that computing g^{ab} from g^a and g^b alone is at least as hard as solving the discrete logarithm problem.

Remarks

- Note that it is not strictly necessary that g be a generator. We can work with any random element of $\mathbb{F}_q^*$ for g, and everything works.
- Security may be compromised if the order of the chosen g is too small, since that would make the discrete logarithm problem easier to solve by a brute-force search.
- However, if $\varphi(q-1)$ is fairly large relative to q then the chance of getting a primitive root by choosing a random element is fairly good.
- In general, I would try to choose q to be one more than a prime. For instance, $q = 2^7 = 128$ satisfies this property, since 127 is prime. Thus there are $\varphi(127) = 126$ primitive roots in $\mathbb{F}_{128}$.

The ElGamal Cryptosystem in $\mathbb{F}_q$

- Fix a finite field $\mathbb{F}_q$ for q very large. Choose some $g \in \mathbb{F}_q^*$, preferably a primitive root.
- Assume that plaintext message units somehow correspond to elements of $\mathbb{F}_q$.
- The number q and the polynomial g are public. Every user U chooses at random an integer $a = a_U$ in the range from 1 to $q - 1$. This is the secret decryption key. The user computes g^a using successive squaring mod $p(x)$ where $p(x)$ is the defining irreducible polynomial for $\mathbb{F}_q$, and publishes the resulting polynomial. The residue g^a is the public key for that user.
- To send a secret message to user U, one chooses an integer k at random, and computes and sends the pair $(\beta_1 = g^k, \beta_2 = P(g^a)^k)$ of residues, where $P \in \mathbb{F}_q$ is a plaintext message unit.

The ElGamal Cryptosystem in $\mathbb{F}_q$

- User U decrypts the received message (β_1, β_2) by computing

$$P = (Pg^{ak})(g^{ak})^{-1} = \beta_2(\beta_1)^{-a}.$$

- The inverse of $\beta_1^a = g^{ak}$ is easily computable by successive squaring, since the calculation

$$(g^{ak})(g^k)^{q-1-a} = (g^k)^a(g^k)^{q-1-a} = (g^k)^{q-1} = 1$$

  proves that $(g^{ak})^{-1} = (g^k)^{q-1-a}$.
- Thus decryption involves nothing but multiplications in $\mathbb{F}_q$ and the successive squaring algorithm, and so decryption uses no more resources than encryption.
- For an attacker to break ElGamal, it is believed that it would be necessary to solve the discrete logarithm problem to find a from the public key $g^a \in \mathbb{F}_q$.