MATH 415

Modern Algebra I

Lecture 18:
Public key encryption.
Rings of polynomials.
Division of polynomials.

Public key encryption

Suppose that Alice wants to obtain some confidential information from Bob, but they can only communicate via a public channel (meaning all that is sent may become available to third parties, in particular, to Eve). How to organize secure transfer of data in these circumstances?

The **public key encryption** is a solution to this problem.

Public key encryption

The first step is **coding**. Bob digitizes the message and breaks it into blocks $b_1, b_2, \ldots, b_k$ so that each block can be encoded by an element of a set $X = \{1, \ldots, K\}$, where K is large. This results in a **plaintext**. Coding and decoding are standard procedures known to public.

Next step is **encryption**. Alice sends a **public key**, which is an invertible function $f : X \to Y$, where Y is an equally large set. Bob uses this function to produce an encrypted message (**ciphertext**): $f(b_1), f(b_2), \ldots, f(b_k)$. The ciphertext is then sent to Alice.

The remaining steps are **decryption** and **decoding**. To decrypt the encrypted message (and restore the plaintext), Alice applies the inverse function f^{-1} to each block. Finally, the plaintext is decoded to obtain the original message.

Trapdoor function

For a successful encryption, the function f has to be the so-called **trapdoor function**, which means that f is easy to compute while f^{-1} is hard to compute unless one knows special information ("trapdoor").

The usual approach is to have a family of functions $f_\alpha : X_\alpha \to X_\alpha$ (where $X \subset X_\alpha$) depending on a parameter α (or several parameters). For any function in the family, the inverse also belongs to the family. The parameter α is the trapdoor.

An additional step in exchange of information is **key generation**. Alice generates a pair of **keys**, i.e., parameter values, α and β such that the function f_β is the inverse of f_α.
α is the **public key**, it is communicated to Bob (and anyone else who wishes to send encrypted information to Alice).
β is the **private key**, only Alice knows it.

The encryption system is efficient if it is virtually impossible to find β when one only knows α.

Modular arithmetic

Fermat's Little Theorem If p is a prime number then $a^{p-1} \equiv 1 \mod p$ for any integer a that is not a multiple of p.

Euler's Theorem If n is a positive integer and $\phi(n)$ is the number of integers between 1 and n coprime with n, then $a^{\phi(n)} \equiv 1 \mod n$ for any integer a coprime with n.

Theorem Let $n > 1$ be an integer and $n = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$ be its prime factorization. Then $\phi(n) = p_1^{s_1 - 1}(p_1 - 1) p_2^{s_2 - 1}(p_2 - 1) \ldots p_k^{s_k - 1}(p_k - 1)$.

RSA system

The **RSA (Rivest-Shamir-Adleman)** system is a public key system based on the modular arithmetic.

$X = \{1, 2, \ldots, K\}$, where K is a large number (say, 2^{128}).

The **key** is a pair of integers (n, α), **base** and **exponent**. The domain of the function $f_{n,\alpha}$ is G_n, the set of invertible congruence classes modulo n, regarded as a subset of $\{0, 1, 2, \ldots, n-1\}$. We need to pick n so that the numbers $1, 2, \ldots, K$ are all coprime with n.

The function is given by $f_{n,\alpha}(a) = a^\alpha \bmod n$.

Key generation: First we pick two distinct primes p and q greater than K and let $n = pq$. Secondly, we pick an integer α coprime with $\phi(n) = (p-1)(q-1)$. Thirdly, we compute β, the inverse of α modulo $\phi(n)$.

Now the public key is (n, α) while the private key is (n, β).

By construction, $\alpha\beta = 1 + \phi(n)k$, $k \in \mathbb{Z}$. Then

$$f_{n,\beta}(f_{n,\alpha}(a)) = [a]_n^{\alpha\beta} = [a]_n([a]_n^{\phi(n)})^k,$$

which equals $[a]_n$ by Euler's theorem. Thus $f_{n,\beta} = f_{n,\alpha}^{-1}$.

Efficiency of the RSA system is based on impossibility of efficient prime factorisation (at present time).

Example. Let us take $p = 5$, $q = 23$ so that the base is $n = pq = 115$. Then $\phi(n) = (p-1)(q-1) = 4 \cdot 22 = 88$.

Exponent for the public key: $\alpha = 29$. It is easy to observe that -3 is the inverse of 29 modulo 88:

$$(-3) \cdot 29 = -87 \equiv 1 \bmod 88.$$

However the exponent is to be positive, so we take $\beta = 85$ ($\equiv -3 \bmod 88$).

Public key: $(115, 29)$, private key: $(115, 85)$.

Example of plaintext: 6/8 (two blocks).

Ciphertext: 26 ($\equiv 6^{29} \bmod 115$), 58 ($\equiv 8^{29} \bmod 115$).

Polynomials in one indeterminate

Definition. A **polynomial** in an indeterminate (or variable) X over a ring R is an expression of the form

$$p(X) = c_0X^0 + c_1X^1 + c_2X^2 + \cdots + c_nX^n,$$

where $c_0, c_1, \ldots, c_n$ are elements of the ring R (called **coefficients** of the polynomial). The **degree** $\deg(p)$ of the polynomial $p(X)$ is the largest integer k such that $c_k \neq 0$. The set of all such polynomials is denoted $R[X]$.

Remarks on notation. The polynomial is denoted $p(X)$ or p. The terms c_0X^0, c_1X^1 and $1X^k$ are usually written as c_0, c_1X and X^k. Zero terms $0X^k$ are usually omitted. Also, the terms may be rearranged, e.g., $p(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots$ $\cdots + c_1X + c_0$. This does not change the polynomial.

Remark on formalism. Formally, a polynomial $p(X)$ is determined by an infinite sequence $(c_0, c_1, c_2, \ldots)$ of elements of R such that $c_k = 0$ for k large enough.

Algebra of polynomials over a field

First consider polynomials over a field $\mathbb{F}$. If

$$p(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$
$$q(X) = b_0 + b_1 X + b_2 X^2 + \cdots + b_m X^m,$$

then $(p+q)(X) = (a_0+b_0) + (a_1+b_1)X + \cdots + (a_d+b_d)X^d$, where $d = \max(n,m)$ and missing coefficients are assumed to be zeros. Also, $(\lambda p)(X) = (\lambda a_0) + (\lambda a_1)X + \cdots + (\lambda a_n)X^n$ for all $\lambda \in \mathbb{F}$. This makes $\mathbb{F}[X]$ into a vector space over $\mathbb{F}$, with a basis $X^0, X^1, X^2, \dots, X^n, \dots$

Further, $(pq)(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{n+m} X^{n+m}$, where $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0$, $k \geq 0$. Equivalently, the product pq is a bilinear function defined on elements of the basis by $X^n X^m = X^{n+m}$ for all $n, m \geq 0$. Multiplication is associative, which follows from bilinearity and the fact that $(X^n X^m) X^k = X^n (X^m X^k)$ for all $n, m, k \geq 0$.

Thus $\mathbb{F}[X]$ is a commutative ring and an associative $\mathbb{F}$-algebra.

Ring of polynomials

Now consider polynomials over an arbitrary ring R. If

$$p(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$
$$q(X) = b_0 + b_1 X + b_2 X^2 + \cdots + b_m X^m,$$

then $(p+q)(X) = (a_0+b_0) + (a_1+b_1)X + \cdots + (a_d+b_d)X^d$, where $d = \max(n, m)$ and missing coefficients are assumed to be zeros. Also, $(\lambda p)(X) = (\lambda a_0) + (\lambda a_1)X + \ldots + (\lambda a_n)X^n$ for all $\lambda \in R$. This makes $R[X]$ into a **module over** R. If $1 \in R$, the module has a basis $X^0, X^1, X^2, \ldots, X^n, \ldots$ (a **free module**).

Further, $(pq)(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{n+m} X^{n+m}$, where $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0$, $k \geq 0$. One can show that multiplication is associative and distributes over addition. Now $R[X]$ is a **ring of polynomials**. If R is commutative (a domain, a ring with unity), then so is $R[X]$.

Notice that $\deg(p \pm q) \leq \max(\deg(p), \deg(q))$. If $p, q \neq 0$ and R is a domain, then $\deg(pq) = \deg(p) + \deg(q)$.

Polynomials in several variables

The ring $R[X, Y]$ of polynomials in two variables X and Y over a ring R can be defined in several ways. We can define it via "currying" as $R[X][Y]$ (that is, polynomials in Y over the ring $R[X]$) or $R[Y][X]$ (that is, polynomials in X over the ring $R[Y]$).

Also, we can define $R[X, Y]$ directly as the set of expressions of the form

$$c_1 X^{n_1} Y^{m_1} + c_2 X^{n_2} Y^{m_2} + \cdots + c_k X^{n_k} Y^{m_k},$$

where each $c_i \in R$, each n_i and m_i is a nonnegative integer, and the pairs (n_i, m_i) are all distinct.

Similarly, we can define the ring $R[X_1, X_2, \ldots, X_n]$ of polynomials in n variables over R.

Division of polynomials

Let $f(x), g(x) \in \mathbb{F}[x]$ be polynomials over a field $\mathbb{F}$ and $g \neq 0$. We say that $g(x)$ **divides** $f(x)$ if $f = qg$ for some polynomial $q(x) \in \mathbb{F}[x]$. Then q is called the **quotient** of f by g.

Let $f(x)$ and $g(x)$ be polynomials and $\deg(g) > 0$. Suppose that $f = qg + r$ for some polynomials q and r such that $\deg(r) < \deg(g)$ or $r = 0$. Then r is the **remainder** and q is the (partial) **quotient** of f by g.

Note that $g(x)$ divides $f(x)$ if the remainder is 0.

Theorem Let $f(x)$ and $g(x)$ be polynomials and $\deg(g) > 0$. Then the remainder and the quotient of f by g are well defined. Moreover, they are unique.

Long division of polynomials

Problem. Divide $x^4 + 2x^3 - 3x^2 - 9x - 7$ by $x^2 - 2x - 3$.

$$
\begin{array}{r|rrrrrrrrr}
 & x^2 & + & 4x & + & 8 & & & & \\
\hline
x^2 - 2x - 3 & x^4 & + & 2x^3 & - & 3x^2 & - & 9x & - & 7 \\
 & x^4 & - & 2x^3 & - & 3x^2 & & & & \\
\hline
 & & & 4x^3 & & & - & 9x & - & 7 \\
 & & & 4x^3 & - & 8x^2 & - & 12x & & \\
\hline
 & & & & & 8x^2 & + & 3x & - & 7 \\
 & & & & & 8x^2 & - & 16x & - & 24 \\
\hline
 & & & & & & & 19x & + & 17
\end{array}
$$

We have obtained that

$x^4 + 2x^3 - 3x^2 - 9x - 7 = x^2(x^2 - 2x - 3) + 4x^3 - 9x - 7$,
$4x^3 - 9x - 7 = 4x(x^2 - 2x - 3) + 8x^2 + 3x - 7$, and
$8x^2 + 3x - 7 = 8(x^2 - 2x - 3) + 19x + 17$. Therefore

$x^4 + 2x^3 - 3x^2 - 9x - 7 = (x^2 + 4x + 8)(x^2 - 2x - 3) + 19x + 17.$

Polynomial expression vs. polynomial function

Let us consider the polynomial ring $\mathbb{F}[X]$ over a field $\mathbb{F}$. By definition, $p(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0 \in \mathbb{F}[X]$ is just an expression. However we can evaluate it at any $\alpha \in \mathbb{F}$ to $p(\alpha) = c_n \alpha^n + c_{n-1} \alpha^{n-1} + \cdots + c_1 \alpha + c_0$, which is an element of $\mathbb{F}$. Hence each polynomial $p(X) \in \mathbb{F}[X]$ gives rise to a **polynomial function** $p : \mathbb{F} \to \mathbb{F}$. One can check that $(p+q)(\alpha) = p(\alpha) + q(\alpha)$ and $(pq)(\alpha) = p(\alpha) q(\alpha)$ for all $p(X), q(X) \in \mathbb{F}[X]$ and $\alpha \in \mathbb{F}$.

Theorem All polynomials in $\mathbb{F}[X]$ are uniquely determined by the induced polynomial functions if and only if $\mathbb{F}$ is infinite.

Idea of the proof: Suppose $\mathbb{F}$ is finite, $\mathbb{F} = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$. Then a polynomial $p(X) = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_k)$ gives rise to the same function as the zero polynomial.

If $\mathbb{F}$ is infinite, then any polynomial of degree at most n is uniquely determined by its values at $n+1$ distinct points of $\mathbb{F}$.

Zeros of polynomials

Definition. An element $\alpha \in \mathbb{F}$ is called a **zero** (or a **root**) of a polynomial $f \in \mathbb{F}[x]$ if $f(\alpha) = 0$.

Theorem $\alpha \in \mathbb{F}$ is a zero of $f \in \mathbb{F}[x]$ if and only if the polynomial $f(x)$ is divisible by $x - \alpha$.

Idea of the proof: The remainder after division of $f(x)$ by $x - \alpha$ is $f(\alpha)$.

Problem. Find the remainder after division of $f(x) = x^{100}$ by $g(x) = x^2 + x - 2$.

We have $x^{100} = (x^2 + x - 2)q(x) + r(x)$, where $r(x) = ax + b$ for some $a, b \in \mathbb{R}$. The polynomial g has zeros 1 and -2. Evaluating both sides at $x = 1$ and $x = -2$, we obtain $f(1) = r(1)$ and $f(-2) = r(-2)$. This gives rise to a system of linear equations $a + b = 1$, $-2a + b = 2^{100}$. Unique solution: $a = (1 - 2^{100})/3$, $b = (2^{100} + 2)/3$.