University of Maryland
CMSC 456 — Introduction to Cryptography
Professor Jonathan Katz

Notes on Algebra and Number Theory[1]
Part 1

The following are brief notes covering several topics in algebra and number theory which will be useful for the course and for applications in cryptography in general. The presentation is informal, and proofs are not given. More thorough treatment can be found in [1, 3, 4].

1 Groups

Definition 1 A group $(G, \cdot)$ is a set G along with an operation $\cdot$ on pairs of elements of G such that the following conditions hold:

1. For all $a, b \in G$, $a \cdot b \in G$.
2. The operation is *associative*: i.e., for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. There exists an *identity element* I such that, for all a, $I \cdot a = a \cdot I = a$.
4. For all $a \in G$ there exists a unique *inverse* $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = I$.

Furthermore, we say a group is *commutative* if, for all $a, b \in G$, $a \cdot b = b \cdot a$. ■

Some common groups include $\mathbb{Z}$, the set of integers under addition, $\mathbb{R}^+$, the set of positive real numbers under addition, and $\mathbb{R}^*$, the set of non-zero real numbers under multiplication. Note that $\mathbb{Z}$ is *not* a group under multiplication (why not?).

For brevity, we denote $a \cdot b$ by ab in a general group, and the notation a^m denotes a multiplied by itself m times. The identity element is typically denoted by e or by 1. We call $|G|$ (i.e., the number of elements in G) the *order* of G. Most of the groups we will deal with in this class will have finite order.

Lemma 1 *Let m be the order of (finite) group G. Then $g^m = 1$ for any nonzero $g \in G$.*

There is a nice (simple) proof for this; see [1] for details.

This simple lemma can be used to demonstrate a very useful fact which we state in its own lemma because it is so important:

Lemma 2 *Let G be a finite group of order m. Let $g \in G$ and x be an integer. Then:*

$$g^x = g^{x \bmod m}.$$

[1] Adapted in part from [2, 3, 5, 6].

Proof Let $x = x' \bmod m$. Then we can write $x = km + x'$. But now we have $g^x = g^{km+x'} = g^{km}g^{x'} = (g^m)^k g^{x'} = (1)^k g^{x'} = g^{x'}$. ■

One type of group which will come up again and again in cryptography (and computer science, generally) is the group of *integers modulo* N, for some integer N. For any integer i, define $i \bmod N$ as the remainder when i is divided by N. Note that, by definition, this means that we have $i \in \{0, \ldots, N-1\}$. Define the group $\mathbb{Z}_N$ as the set $\{0, \ldots, N-1\}$ under addition, where addition is done by adding elements of $\mathbb{Z}_N$ "normally" (i.e., over the integers) and then reducing modulo N. For example, if we are working in $\mathbb{Z}_5$, then $4 + 3 = 2 \bmod 5$. When the underlying group is clear from the context, we will simply write $4 + 3 = 2$. Note that the validity of such a statement depends tremendously on the underlying group!

Note that $\mathbb{Z}_N$ is *not* necessarily a group under multiplication; for example, in $\mathbb{Z}_{15}$ the element 5 has no (multiplicative) inverse. We can "fix" this, however, by introducing a commutative group which will be of great importance in our study of cryptography:

Lemma 3 *Let N be an integer, and define $\mathbb{Z}_N^* = \{m : 1 \leq m \leq N \text{ and } \gcd(m, N) = 1\}$. Then $\mathbb{Z}_N^*$ is a group under multiplication (modulo N).*

Definition 2 We denote $|\mathbb{Z}_N^*|$ by $\varphi(N)$. Thus, $\varphi(N)$ is the number of elements of $\mathbb{Z}_N^*$. ■

If p is prime, one can show that $\varphi(p) = p - 1$ (this is because $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ in this case). Another important case is when N as the product of two distinct primes p, q; i.e., $N = pq$. In this case, one can show by a simple counting argument that $\varphi(N) = (p-1)(q-1)$.

2 Fields

A *field* is an extension of the concept of a group.

Definition 3 A field $(F, +, \times)$ is a set F with special elements 0 and 1, along with two operations $(+, \times)$ defined on pairs of elements of F such that the following conditions hold:

1. $(F, +)$ is a commutative group, with identity the element 0.
2. The $\times$ operation is associative; for all $a, b, c \in F$, $a \times (b \times c) = (a \times b) \times c$.
3. The $\times$ operation is commutative: for all $a, b \in F$, $a \times b = b \times a$.
4. The element 1 is an identity for $\times$; for all $a \in F$, $1 \times a = a \times 1 = a$.
5. The *distributive law* is satisfied; for all $a, b, c \in F$, $a \times (b + c) = (a \times b) + (a \times c)$.
6. All nonzero elements in F have an inverse under $\times$; for all $a \in F, a \neq 0$, there exists an element $a^{-1} \in F$ such that $a \times a^{-1} = 1$.

■

For any field F, we denote by F^* the set of nonzero elements of F. Thus, every element of F^* has an inverse. As an example, $\mathbb{Z}_p^*$ for p prime (see below) is the set $\{1, \ldots, p-1\}$.

Note that $\mathbb{Z}_5$ is a field, under addition and multiplication modulo 5. To see this, note that we already know that $\mathbb{Z}_5$ is a group under addition (from Section 1). Furthermore, we can check that requirements 2–5 are satisfied (since they hold over the set $\{1, \ldots, 5\}$ considered over the integers, this essentially implies that they hold). The non-trivial one to check is condition 6, but this can be verified on a case-by-case basis (i.e., the inverse of 2 is 3; 4 is its own inverse). On the other hand, note that $\mathbb{Z}_6$ is *not* a field. For example, 4 has no multiplicative inverse (try to find one!).

There is one type of field which we will be concerned with in this class; this is the subject of the following lemma. Before presenting the lemma, we remind the reader that a *prime number* is an integer $p \geq 2$ whose only divisors are 1 and p.

Lemma 4 *Let p be a prime number. Then $\mathbb{Z}_p$ is a field under addition and multiplication modulo p.*

3 Complexity of Arithmetic Operations

In cryptography, we tend to deal with large numbers (on the order of 2^{512}) so it is worth stepping back and making sure that arithmetic operations on these integers can be done efficiently. Recall that the efficiency of an algorithm operating on a number a is not measured in terms of a but rather in terms of the length (number of bits) in a, written here as $|a| = \lceil \log_2 a \rceil$. Fortunately, all "simple" arithmetic operations can be done in polynomial time in the length of the inputs. We state the following facts without proof (in the following, a, b are positive integers with $a \geq b$):

1. Addition of a and b can be done in time $O(|a|)$.
2. Multiplication of a and b can be done in time $O(|a| \cdot |b|)$. In fact, this can be improved to $O(|a| \cdot \log |a| \cdot \log \log |a|)$.
3. Division of a by b (returning both the quotient and the remainder) can be done in time $O(|a| \cdot |b|)$. Note this means that we can compute $a \bmod b$ in time $O(|a| \cdot |b|)$. This can be also improved.

What about exponentiation? We will only be interested in exponentiation modulo some fixed value N (so that, in particular, our final answer will always be bounded by N), so the question becomes: how fast can we compute $a^b \bmod N$? A very naive way of doing this is to compute $a^2 = a \cdot a; a^3 = a \cdot a^2, \ldots, a^b = a \cdot a^{b-1}$ and then finally reduce a^b modulo N (what is the time required for this approach?). A somewhat less naive method is to reduce the value at each step; i.e., compute $a^2 \bmod N = a \cdot a \bmod N; a^3 \bmod N = a \cdot a^2 \bmod N, \ldots$. Note, however, that this algorithm has b steps so the running time will be exponential in $|b|$!

A more careful algorithm — *repeated squaring* — is needed. Pseudocode for this algorithm follows (we assume $b \geq 0$ for simplicity):

```
Input: a, b, N
  if (b = 0) return 1
  ans = a, tmp = 1
  // we maintain the invariant that our solution is tmp * ans^b mod N
  while (b > 1) {
    if (b is odd) {
      tmp = tmp * ans mod N
      b = b - 1 }
    ans = ans * ans mod N
    b = b/2 }
  return (tmp * ans mod N)
```

Note that this algorithm performs at most $2|b|$ multiplications and each multiplication takes time $O(|N|^2)$ (we assume here that $a < N$ — if this is not the case we reduce a before starting). So the total running time of the algorithm is $O(|b| \cdot |N|^2)$.

We state without proof the fact that the greatest common divisor of a and b can be computed in time $O(|a| \cdot |b|)$ (this uses *Euclid's algorithm*). In fact, we can do even better using the *extended Euclid's algorithm*: in the same time bound we can compute natural numbers m, n (with $-a/2 \leq m, n \leq a/2$) such that $ma + nb = \gcd(a, b)$. This fact turns out to be surprisingly useful; as an example, consider the problem of computing the inverse of an element $a \in \mathbb{Z}_N^*$. By definition of $\mathbb{Z}_N^*$, we know that $\gcd(a, N) = 1$. Thus, using the extended Euclid's algorithm we can find n, m such that $na + mN = 1$ (note that one of n, m may be negative). But now, we claim that n is the inverse we desire. Indeed, we have: $na = 1 - mN = 1 \bmod N$. Thus, $n = a^{-1} \bmod N$.

4 Chinese Remainder Theorem

A very useful algorithmic result is the following (we say two integers N_1, N_2 are co-prime if $\gcd(N_1, N_2) = 1$):

Theorem 1 *Consider a system of equations of the form:*

$$\begin{aligned} x &= a_1 \bmod N_1 \\ x &= a_2 \bmod N_2 \\ &\vdots \\ x &= a_k \bmod N_k. \end{aligned}$$

where x is the variable and $a_1, \ldots, a_n$ and $N_1, \ldots, N_k$ are given. Suppose $N_1, \ldots, N_k$ are pairwise co-prime. Then there is always a unique *solution x, with $0 \leq x < N_1 \cdots N_k$. Furthermore, such x is efficiently computable given $a_1, \ldots, a_n$ and $N_1, \ldots, N_k$. Finally, the set of all solutions are the integers y such that $y = x \bmod N_1 \cdots N_k$.*

Assume $N = pq$, with p, q prime (note that this implies that p and q are co-prime). The above theorem gives an alternate way to represent elements of $\mathbb{Z}_N$: we may represent $x \in \mathbb{Z}_N$ by the pair (a, b) with $a \in \mathbb{Z}_p$ and $b \in \mathbb{Z}_q$, where $x = a \bmod p$ and $x = b \bmod q$.

For example, $7 \in \mathbb{Z}_{15}$ can be written as $(1, 2)$ since $7 = 1 \bmod 3$ and $7 = 2 \bmod 5$. An important property of these representations is given by the following fact:

Fact 1 *Let $N = pq$, with p, q prime. Let $x \leftrightarrow (x_p, x_q)$ be the representation described above. Then:*

- *If $x + y = z \bmod N$ then $(x_p, x_q) + (y_p, y_q) = (z_p, z_q)$, where: $z_p = x_p + y_p \bmod p$ and $z_q = x_q + y_q \bmod q$.*
- *If $xy = z \bmod N$ then $(x_p, x_q) \cdot (y_p, y_q) = (z_p, z_q)$, where: $z_p = x_p y_p \bmod p$ and $z_q = x_q y_q \bmod q$.*

We give an example of some very useful facts one can derive from this simple observation. First, note that this gives a quick "proof" that $\varphi(N) = (p-1)(q-1)$ when $N = pq$ and p, q are prime. Indeed, represent elements as above. Then $(a, b) \in \mathbb{Z}_N^*$ iff (a, b) is not divisible by p and not divisible by q. But note that (a, b) is divisible by p exactly when $a = 0$, and similarly is divisible by q exactly when $q = 0$. Thus, the number of elements (a, b) which are in $\mathbb{Z}_N^*$ is given by all choices of a except 0 and all choices of b except 0, giving $(p-1)(q-1)$ possibilities. Furthermore, note that the inverse of (a, b) in $\mathbb{Z}_N^*$ is given by (a^{-1}, b^{-1}), where a^{-1} is the inverse of a in $\mathbb{Z}_p$, etc.

Let's now look at elements which are *squares* in $\mathbb{Z}_p$, where $p \geq 3$ is prime (note: an element a is a square if $a = x^2 \bmod p$ for some x). We claim that every element in $\mathbb{Z}_p$ has either no square roots (i.e., is not a square) or exactly two distinct square roots. As an informal proof (note that all calculations in this paragraph are implicitly done in the group $\mathbb{Z}_p$), note that if an element a has a square root x, then $-x$ is also a square root of a. Furthermore, x and $-x$ are distinct modulo p when p is odd (why?) — note that is not true for the case when $p = 2$ which is why we excluded it above. So, any element which is a square has at least two square roots. Can there be more? Well, let x and y be square roots of a. Then $x^2 = y^2$ and thus: $x^2 - y^2 = 0$. Algebra gives: $(x - y)(x + y) = 0$. But this has the two solutions $x = y$ and $x = -y$ (important note: this makes use of the fact that the equation $wz = 0$ has solutions only if $w = 0$ or $z = 0$, or both. This is true for $\mathbb{Z}_p$, which is a field. This is not, in general, true for all groups, as we will see below). As an aside, note that this also gives us a count of how many squares there are in $\mathbb{Z}_p$. Since every square maps to two, distinct elements of the group, exactly half of the nonzero elements of $\mathbb{Z}_p$ must be squares (i.e., $(p-1)/2$).

We now consider $\mathbb{Z}_N$, where $N = pq$, and p and q are prime. How many square roots can elements have now? We show that each element has either no square roots or exactly *four* distinct square roots. We work with the representations of elements of $\mathbb{Z}_N$ given by the Chinese remainder theorem above. Consider an element (a, b). A little thought shows that (a, b) is a square iff a is a square *and* b is a square. Then the four square roots of (a, b) are given by: $(\sqrt{a}, \sqrt{b})$, $(-\sqrt{a}, \sqrt{b})$, $(\sqrt{a}, -\sqrt{b})$, and $(-\sqrt{a}, -\sqrt{b})$. Furthermore, this shows that the number of squares in $\mathbb{Z}_N^*$ is $1/4$ of the the elements of $\mathbb{Z}_N^*$.

(As an aside, note why the proof that there are only two square roots given in the case of $\mathbb{Z}_p$, p prime, fails here. In particular, it is not the case that if $xy = 0 \bmod N$ then either $x = 0$ or $y = 0$. As an easy counterexample, note that, for any a, b we have [using representations]: $(a, 0) \cdot (0, b) = (0, 0) = 0$.)

It is the case that square roots modulo prime p can be computed in polynomial-time. Note that this allows efficient calculation of square roots modulo N *if* the factors of N are known (by application of the Chinese remainder theorem). We will show later (in class) that square roots cannot be computed in polynomial time modulo N without knowing the factorization of N, unless factoring can be done in polynomial time.

5 Legendre and Jacobi Symbols, Quadratic Residuosity

Notation has developed for dealing with quadratic residues in modular groups. For elements in $\mathbb{Z}_p^*$ (p prime), we call an element which is a square a *quadratic residue*, and define the Legendre symbol as follows:

$$\mathcal{L}_p(y) = \begin{cases} +1 & \text{if } y \text{ is a quadratic residue modulo } p \\ 0 & \text{if } y = 0 \\ -1 & \text{otherwise.} \end{cases}$$

We can extend this definition to the case $N = pq$ (p, q prime), and define the Jacobi symbol as follows:

$$\mathcal{J}_N(y) = \mathcal{L}_p(y) \cdot \mathcal{L}_q(y).$$

Note that if y is a square in $\mathbb{Z}_N$, then we must have $\mathcal{J}_N(y) = +1$. This is so because if x is a square modulo N, and $x \leftrightarrow (a, b)$, then a must be a square modulo p and b must be a square modulo q. On the other hand, there are elements y with $\mathcal{J}_N(y) = +1$ which are *not* quadratic residues; these are precisely those elements $y \leftrightarrow (a, b)$ where neither a nor b are squares (and hence $\mathcal{L}_p(a) = \mathcal{L}_q(b) = -1$).

An important result is that the Jacobi symbol of x modulo N can be efficiently computed *even if the factorization of N is not known*. Thus, if we compute $\mathcal{J}_N(x) = -1$ we know that x cannot be a quadratic residue. On the other hand, given an element x for which $\mathcal{J}_N(x) = +1$ and without the factorization of N, no efficient algorithm is known to determine whether x is a quadratic residue or not. We will use this in building an encryption scheme later in the course.

6 Generators

Generators are special elements that exist in certain groups.

Definition 4 Let G be a group of order n, let $g \in G$, and suppose that $g^1, g^2, \ldots, g^n$ are all distinct (note that, in this case, we have $\{g^1, \ldots, g^n\} = G$). Then G is said to be *cyclic* and g is said to be a *generator* of G. ■

Examples of cyclic groups include $\mathbb{Z}_N$, for arbitrary N, under addition. More interesting are groups which are cyclic under multiplication.

Theorem 2 *For every prime, $\mathbb{Z}_p^*$ is a cyclic group under multiplication.*

Note that even in a cyclic group, not every element is a generator.

For cryptographic purposes, an important example of a cyclic group is the following. Let $p = 2q + 1$ with p, q prime (such primes can be efficiently found). We state without proof the fact that there is a subgroup G of $\mathbb{Z}_p^*$ which is of order q; furthermore, this subgroup is cyclic. Finally, a generator g of this subgroup can be efficiently found and given g we can efficiently tell whether it is a generator of this subgroup (see [3, Section B.5] for more details).

In this group (actually, this holds for any group), computation in the exponent can be done modulo the order of the group. Thus, $g^i \bmod p = g^{i \bmod q} \bmod p$, etc. Also, in a cyclic group, discrete logarithms are well-defined with respect to any generator. For example, if g is a generator of G, then for any element $h \in G$, we know that $g^i = h$ for some i. Furthermore, this i is unique (modulo the order of the group q). We denote this unique value i by $\log_g(h)$, where the underlying group G is understood from the context.

7 Conjectured Hard Problems

I.e., RSA, factoring (squaring), and discrete logarithm

8 Primality Testing

To come...

References

[1] L.N. Childs. *A Concrete Introduction to Higher Algebra (Second Edition)*. Springer, 1995.

[2] C. Crépeau. Lecture Notes for Computer Science 308-547A: Cryptography and Data Security, pp. 33–45.

[3] S. Goldwasser and M. Bellare. *Lecture Notes on Cryptography*, Appendix B. June, 1997.

[4] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbook on Applied Cryptography*, Chapters 2–3. CBC Press, 1996.

[5] L. Trevisan. *Notes on Algebra*, January, 1999.

[6] L. Trevisan. *Notes on Number-Theoretic Algorithms*, December, 1999.