PMAT 4282 – Cryptography — Assignment #5
Winter 2001

A *group* $(\mathcal{G}, \cdot)$ consists of a set $\mathcal{G}$ along with a binary operation $\cdot$, such that:

- $\mathcal{G}$ is closed under $\cdot$
- $\cdot$ is associative (ie. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$)
- there exists an identity with respect to $\cdot$
  (ie. there exists an element $e \in \mathcal{G}$ such that $a \cdot e = e \cdot a = a$ for all $a \in \mathcal{G}$)
- each element has an inverse
  (ie. for each $a \in \mathcal{G}$ there exists an element $b \in \mathcal{G}$ such that $a \cdot b = b \cdot a = e$)

Note that we often refer to the group as $\mathcal{G}$ rather than $(\mathcal{G}, \cdot)$. Notice also that $\cdot$ need not be commutative; a group in which $\cdot$ is commutative is called an *Abelian* group.

The notation a^n will be used to denote $\underbrace{a \cdot a \cdot a \cdots a}_{n\ a\text{'s}}$. The *order* of an element $a \in \mathcal{G}$ is the smallest positive integer t such that $a^t = e$, and if $t = |\mathcal{G}|$ then a is a *generator* of $\mathcal{G}$.

1. Recall that $\mathbb{Z}_n^*$ is the set $\{a \in \mathbb{Z}_n \,|\, \mathrm{GCD}(a, n) = 1\}$. Along with multiplication modulo n, $\mathbb{Z}_n^*$ forms an Abelian group.

   Let $a \in \mathbb{Z}_n^*$. Show that a is a generator of $\mathbb{Z}_n^*$ if and only if the order of a is $\phi(n)$, where ϕ is Euler's totient function.

2. Find all generators of each of the following groups:

   (a) $\mathbb{Z}_9^*$
   (b) $\mathbb{Z}_{15}^*$
   (c) $\mathbb{Z}_{17}^*$
   (d) $\mathbb{Z}_{25}^*$

3. Solve for x (ie find the smallest non-negative integer solution):

   (a) $5^x \equiv 4 \pmod{37}$
   (b) $6^x \equiv 16 \pmod{41}$
   (c) $13^x \equiv 12 \pmod{197}$
   (d) $55^x \equiv 444 \pmod{569}$

4. $\mathrm{GF}(p^k)$, the Galois field of order p^k where p is a prime, is a (actually, it's *the*) field of order p^k. Often the elements of $\mathrm{GF}(p^k)$ are chosen to be all polynomials, with coefficients in $\mathbb{Z}_p$, of degree less than k. Addition of two elements is done in the normal way that we would add polynomials, except that the numerical coefficients are added modulo p. Likewise, multiplication of two elements involves reducing the coefficients modulo p, but is also done modulo an irreducible polynomial $m(x)$ of degree k (a polynomial is said to be irreducible if it has no divisors other than 1 and itself).

   For example, if $a = x^4 + x^3 + x + 1$ and $b = x^4 + x + 1$, then $ab = x^8 + x^7 + x^4 + x^3 + x^2 + 1$ when working over $\mathbb{Z}_2$. When reduced modulo $x^3 + x + 1$, $ab = x + 1$.

(a) Find all of the irreducible polynomials of degree 1 over $\mathbb{Z}_2$.

(b) Find all of the irreducible polynomials of degree 2 over $\mathbb{Z}_2$.

(c) Find all of the irreducible polynomials of degree 3 over $\mathbb{Z}_2$.

(d) Is $x^4 + x^2 + x + 1$ irreducible over $\mathbb{Z}_2$?

(e) Is $x^4 + x^3 + 1$ irreducible over $\mathbb{Z}_2$?

(f) Is $x^4 + x^2 + 1$ irreducible over $\mathbb{Z}_2$?

(g) Consider the field $\mathcal{F} = \mathrm{GF}(2^4)$, with $m(x) = x^4 + x + 1$. Calculate:

   i. $(x^2 + x + 1)^2$

   ii. $(x + 1)^4$

   iii. $(x^3 + x + 1)^2(x^2 + 1)$

Note that the Rijndael cipher (which was adopted by NIST in October 2000 as the new Advanced Encryption Standard (AES)) uses $\mathrm{GF}(2^8)$ with $m(x) = x^8 + x^4 + x^3 + x + 1$.