Scribe Notes for *Algorithmic Number Theory*
Class 17—June 10, 1998

Scribes: Cara Struble and Craig Struble

Abstract

We discuss issues about finding a dth root $\sqrt[d]{a}$ of an element a in $\mathbb{F}_q$. Formulas for finding dth roots when $\gcd(d,q)=1$ and square roots when $q=2^n$ and $q \equiv 3 \pmod 4$ are given. Finally, Tonelli's algorithm for computing square roots in $\mathbb{F}_q$ when q is the power of an odd prime is presented.

1 Preamble

We now look at the problem of finding a dth root of a in a finite field $\mathbb{F}_q$; that is, given $a \in (\mathbb{F}_q)^*$, find an $x \in (\mathbb{F}_q)^*$ such that $x^d = a$. $(\mathbb{F}_q)^*$ is a cyclic group of order $r = q-1$. Since cyclic groups of the same order are isomorphic, we study the cyclic group $C_r = \{\overline{0}, \overline{1}, \ldots, \overline{r-1}\} \cong \mathbb{Z}/(r)$ as an additive group. Let $f_d : C_r \to C_r$ be the following map,

$$f_d(c) = d \cdot c = \underbrace{c + c + \cdots + c}_{d}.$$

There are two cases to consider for finding dth roots in $\mathbb{F}_q$.

1. If $\gcd(d,r)=1$, then f_d is a 1–1 function, that is, a permutation of elements in C_r. Every element of C_r has a unique dth root. Use the extended Euclidean algorithm to find y and z solving the equation

$$yd + zr = 1.$$

   Then, $x = y \cdot a$ is a dth root of a as shown in the following equation:

$$d \cdot (y \cdot a) = (1 - zr) \cdot a = a.$$

2. If $\gcd(d,r) = k > 1$, then f_d is a k to 1 function, that is, a group homomorphism

$$C_r \to C_{r/k}.$$

   In this case, think of first finding a kth root of a, call it b. Second, find a (d/k)th root of b. For b to exist, we must have $k \mid a$. Dividing by k requires that we know a as a multiple of some generator g of C_r,

$$a = \underbrace{g + g + \cdots + g}_{j}.$$

   Then $b = \frac{j}{k} \cdot g$. All of the kth roots are $\left(\frac{j}{k} + \frac{ri}{k}\right) \cdot g$ where $0 \le i < k$.

As an example of this second case, consider when $r = 15$ and $d = 3$. Then the map f_3 is a map from C_{15} to a cyclic subgroup of order 5 isomorphic to C_5. The following table shows the images of f_3, where g is a generator of C_{15}.

x	$f_3(x)$
$0 \cdot g$	$0 \cdot g$
$1 \cdot g$	$3 \cdot g$
$2 \cdot g$	$6 \cdot g$
$3 \cdot g$	$9 \cdot g$
$4 \cdot g$	$12 \cdot g$
$5 \cdot g$	$0 \cdot g$
$6 \cdot g$	$3 \cdot g$
$7 \cdot g$	$6 \cdot g$
$8 \cdot g$	$9 \cdot g$
$9 \cdot g$	$12 \cdot g$
$10 \cdot g$	$0 \cdot g$
$11 \cdot g$	$3 \cdot g$
$12 \cdot g$	$6 \cdot g$
$13 \cdot g$	$9 \cdot g$
$14 \cdot g$	$12 \cdot g$

Notice that $\{0 \cdot g, 3 \cdot g, 6 \cdot g, 9 \cdot g, 12 \cdot g\}$ is a cyclic subgroup of order 5, with $3 \cdot g$ as a generator. Since $C_{15} \cong \mathbb{Z}/(15) \cong \mathbb{Z}/(3) \oplus \mathbb{Z}/(5)$, we can view finding a dth root in C_{15} as independently finding a dth in $\mathbb{Z}/(3)$ and $\mathbb{Z}/(5)$.

2 Square Roots: Group Theoretic Methods

There are two methods of solving the root finding problem that we will study: group theoretic methods and field theoretic methods. Section 7.1 introduces the group theoretic methods for finding dth roots in $\mathbb{F}_q$. This first theorem is a direct consequence of the first case discussed in the preamble.

Theorem 2.1 (Theorem 7.1.1). *Let G be a group of odd order m, written multiplicatively. Let $a \in G$. Then, the equation $x^2 = a$ has a unique solution in G, which is $a^{(m+1)/2}$.*

Proof. Using the notation from the preamble, $d = 2$. Now find a multiplicative inverse of 2 in $\mathbb{Z}/(m)$. That inverse is $\frac{m+1}{2}$. So, $a^{(m+1)/2}$ is the square root of a. □

How expensive is finding a square root in G? Recall that the complexity of exponentiation is $O(s \log m)$ where s is the cost of multiplication. The next corollary shows that in some $(\mathbb{F}_q)^*$ the time complexity of finding a square root is $O((\lg q)^3)$ bit operations.

Corollary 2.2 (Corollary 7.1.2). *If $q = 2^n$ or $q \equiv 3 \pmod 4$, then square roots in $\mathbb{F}_q$ can be computed in $O((\lg q)^3)$ bit operations.*

Proof. First, suppose $q = 2^n$. Then, $q - 1$ is odd, so $gcd(2, q-1) = 1$. $2 \cdot 2^{n-1} \equiv 1 \pmod{2^n - 1}$. So $a^{2^{n-1}}$ is the square root of a.

Now, suppose $q \equiv 3 \pmod 4$. The square map takes $(\mathbb{F}_q)^*$ to a subgroup of order $\frac{q-1}{2}$; that is,

$$f_2 : (\mathbb{F}_q)^* \to ((\mathbb{F}_q)^*)^2.$$

Let g be some generator in $(\mathbb{F}_q)^*$. If a has a square root, then $a \in ((\mathbb{F}_q)^*)^2$ and $a = g^{2i}$. $((\mathbb{F}_q)^*)^2$ has odd cardinality, because $q \equiv 3 \pmod 4$. We want a multiplicative inverse of 2 in $\mathbb{Z}/\left(\frac{q-1}{2}\right)$;

$$\frac{q+1}{4} \cdot 2 = \frac{q+1}{2} \equiv 1 \pmod{(q-1)/2}.$$

Hence, $a^{(q+1)/4}$ is a square root of a. $\square$

Now, consider the more general case of finding square roots in $\mathbb{F}_q$ for any odd q. Write $q = 2^s t$, where $s \geq 1$ and t is odd. Since

$$(\mathbb{F}_q)^* \cong \mathbb{Z}/(2^s) \times \mathbb{Z}/(t),$$

we may write $a = bc$, where $b \in \mathbb{Z}/(2^s)$ and $c \in Z/(t)$. We can use previous results to get $\sqrt{c} = c^{(t+1)/2}$.

Now consider successive applications of f_2 to $(\mathbb{F}_q)^*$. Suppose f_2 is applied s times,

$$\underbrace{(\mathbb{F}_q)^* \xrightarrow{f_2} (\mathbb{F}_q)^* \xrightarrow{f_2} \cdots \xrightarrow{f_2} (\mathbb{F}_q)^*}_{s \text{ times.}}$$

Each map permutes $\mathbb{Z}/(t)$ and halves the image of $\mathbb{Z}/(2^s)$ s times. Thus, considering successive images, we have

$$G_s \xrightarrow{f_2} G_{s-1} \xrightarrow{f_2} \cdots \xrightarrow{f_2} G_0 = H \cong \mathbb{Z}/(t).$$

From this, we get

$$H = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_s = (\mathbb{F}_q)^*.$$

Example 2.3. Suppose $q = 17$, hence $q - 1 = 16 = 2^4 \cdot 1$. Also suppose g generates $(\mathbb{F}_q)^*$. Look at the chain of subgroups from applying f_2 to $(\mathbb{F}_{17})^*$.

$$\begin{aligned} G_4 &= (\mathbb{F}_{17})^* \\ G_3 &= \{g^0, g^2, g^4, g^6, g^8, g^{10}, g^{12}, g^{14}\} \\ G_2 &= \{g^0, g^4, g^8, g^{12}\} \\ G_1 &= \{g^0, g^8\} \\ G_0 &= \{g^0\} \end{aligned}$$

These observations about $(\mathbb{F}_q)^*$ when q is odd lead to Tonelli's Algorithm for finding square roots in $(\mathbb{F}_q)^*$.

3 Tonelli's Algorithm

We continue to use the notation from the previous section, in particular the definitions of s and t. To begin Tonelli's algorithm, choose a random element $z \in (\mathbb{F}_q)^*$ and compute $g = z^t$, which forces the component of z in $\mathbb{Z}/(t)$ to the identity. With probability $\frac{1}{2}$, g is a generator of $\mathbb{Z}/(2^s)$. Assume g is a generator. Then,

$$a = g^e h$$

where $0 \leq e \leq 2^s - 1$ and $h \in H$. Write the binary representation of e,

$$e = e_{s-1}2^{s-1} + e_{s-2}2^{s-2} + \cdots + e_1 2 + e_0$$

where $e_i = \{0, 1\}$.

How do we compute the e_i's? If $a^{(q-1)/2} \neq 1$, then $e_0 = 1$ (which implies a does not have a square root). If $(ag^{-e_0})^{(q-1)/4} \neq 1$, then $e_1 = 1$. If $\left(ag^{-(2e_1+e_0)}\right)^{(q-1)/8} \neq 1$, then $e_2 = 1$. Keep iterating this process to compute each e_i. Algorithmically, we accumulate e as

$$\begin{aligned} e &\leftarrow 0 \\ e &\leftarrow e_0 \\ e &\leftarrow 2e_1 + e_0 \\ e &\leftarrow 4e_2 + 2e_1 + e_0 \\ &\vdots \end{aligned}$$

Tonelli's algorithm is presented as pseudo-code below.

TONELLI(a)
$\triangleright$ Computes $b = \sqrt{a}$ in $(\mathbb{F}_q)^*, q$ odd
let $q - 1 = 2^s t$, where t is odd.
choose a random $z \in (\mathbb{F}_q)^*$
$g \leftarrow z^t$
if $g^{2^{s-1}} = 1$
   then error "g is not a generator of $\mathbb{Z}/(2^s)$"
$e \leftarrow 0$
for $i \leftarrow 0$ **to** $s - 1$
do if $(ag^{-e})^{(q-1)/2^{i+1}} \neq 1$
      then $e \leftarrow e + 2^i$
if $e \bmod 2 = 1$
   then error "a does not have a square root"
$h \leftarrow ag^{-e}$
$b \leftarrow g^{e/2} h^{(t+1)/2}$
return b