Yinghua Wu *November 6, 2006*

Solutions to Problem Set 4

Problem 17: Diffie-Hellman Key Exchange

(a) Recall Lucas test: g is a primitive root of p if and only if

$$g^{(p-1)/q} \not\equiv 1 \pmod{p}$$

for all $q > 1$ such that $q \mid (p-1)$. So here for $p = 29$ and $g = 2$, we check all the possible $q = \{2, 4, 7, 14, 28\}$ as the following:

$$\begin{aligned} 2^{28/2} &\equiv 28 \pmod{29} \\ 2^{28/4} &\equiv 12 \pmod{29} \\ 2^{28/7} &\equiv 16 \pmod{29} \\ 2^{28/14} &\equiv 4 \pmod{29} \\ 2^{28/28} &\equiv 2 \pmod{29} \end{aligned}$$

Therefore, g has passed Lucas test and is a primitive root of p.

(b) According to Diffie-Hellman Key Exchange Protocol, Alice computes $a \equiv g^x \equiv 2^5 \equiv 3 \pmod{p}$, and Bob computes $b \equiv g^y \equiv 2^3 \equiv 8 \pmod{p}$. So the shared secret key is $k \equiv a^y \equiv b^x \equiv 27 \pmod{p}$.

Problem 18: ElGamal Cryptosystem

According to ElGamal Protocol, Bob's public key is $(p, g, b) = (29, 2, 8)$ and private key is $(p, g, y) = (29, 2, 3)$.

Problem 19: Square Roots with Composite Moduli

(a) $|\mathbf{Z}^*_{105}| = \phi(105) = \phi(3) * \phi(5) * \phi(7) = 48$.

(b) Because $105 = 3 \times 5 \times 7$ and $1 \in \mathbf{Z}^*_{105}$, then if $b^2 \equiv 1 \pmod{105}$, we have

$$\begin{aligned} b^2 &\equiv 1 \pmod{3} \\ b^2 &\equiv 1 \pmod{5} \\ b^2 &\equiv 1 \pmod{7} \end{aligned}$$

And we can easily see that the squre roots of 1 in $\mathbf{Z}^*_3$, $\mathbf{Z}^*_5$ and $\mathbf{Z}^*_3$ are all ± 1. Conversely, if there is b satisfying the following equations:

$$\begin{aligned} b &\equiv \pm 1 \pmod{3} \\ b &\equiv \pm 1 \pmod{5} \\ b &\equiv \pm 1 \pmod{7} \end{aligned}$$

Then $b^2 \equiv 1 \pmod{105}$. According to Chinese Remainder theorem, we solve the above set of equations and get all square roots of 1 modulo 105, $\{1, 29, 34, 41, 64, 71, 76, 104\}$.

(c) From (b) and some extension of Claim 1 in Section 62, we could know that the mapping $cu : \mathbf{Z}_n^* \to \mathrm{QR}_n$ defined by $b \longmapsto b^2 \pmod n$ is a 8-to-1 function, in which $n = pqr$ for p, q, r distinct odd primes. The brief explanation is if $a \in \mathrm{QR}_n$, then a has two square roots $S_p = \{\pm b_p\}$ mod p, two square roots $S_q = \{\pm b_q\}$ mod q and two square roots $S_r = \{\pm b_r\}$ mod r. Any triple combination $\{b_1, b_2, b_3\}$, in which $b_1 \in S_p$, $b_2 \in S_q$ and $b_3 \in S_r$, uniquely determines the number $b \in \mathbf{Z}_n^*$ such that $b^2 \equiv a \pmod n$. So cu is a 8-to-1 function and $|\mathrm{QR}_{105}| = \frac{1}{8}|\mathbf{Z}_{105}^*| = 6$.

From the above description, we can know that if $a \in \mathrm{QR}_n$, then a is also a quadratic residue modulo p, q, r, and vice versa. So in order to find out all quadratic residues of $n = 105$, we need to find out quadratic residues of $p = 3, q = 5, r = 7$ first. That's $\mathrm{QR}_3 = \{1\}$, $\mathrm{QR}_5 = \{1, 4\}$, and $\mathrm{QR}_7 = \{1, 2, 4\}$. We solve the following set of equations by Chinese Remainder theorem:

$$\begin{aligned} a &\equiv a_1 \pmod 3), a_1 \in \mathrm{QR}_3 \\ a &\equiv a_2 \pmod 5), a_2 \in \mathrm{QR}_5 \\ a &\equiv a_3 \pmod 7), a_3 \in \mathrm{QR}_7, \end{aligned}$$

and we can get all the quadratic residues module 105, $\{1, 4, 16, 46, 64, 79\}$.

Problem 20: Computing Square Roots Modulo a Prime

(a) According to Euler Criterion, since 103 is a prime and $2^{(103-1)/2} \equiv 2^{51} \equiv (2^{10})^5 * 2 \equiv (-6)^5 * 2 \equiv 1 \pmod{103}$, 2 is a quadratic residue modulo 103.

(b) According to Claim 3 in Section 64, since $103 \equiv 3 \pmod 4$ and $2 \in \mathrm{QR}_{103}$, then $b \equiv 2^{(103+1)/4} \equiv 2^{26} \equiv 38 \pmod{103}$ is a square root of 2 modulo 103.

Problem 21: Quadratic Residues

You can use Legendre Symbol to directly show the result or make advantage of a prime's primitive roots as the following:

Since p is an odd prime, there must be some primitive root of p, denoted as g. Assume $a \equiv g^u \pmod p$ and $b \equiv g^v \pmod p$. Since $a, b \in \mathrm{QNR}_p$, u and v must be odd integers. Then $ab \equiv g^{u+v} \pmod p$. Because $u + v$ is even, $g^{(u+v)/2}$ is exactly a square root of ab. So ab is a quadratic residue modulo p.