Notes on Problem Set 4

3. Stinson, problem 6.17, p.250

We're given

$$\begin{aligned}
y_1 &= x^{b_1} \bmod n && (1)\\
y_2 &= x^{b_2} \bmod n && (2)\\
c_1 &= b_1^{-1} \bmod b_2 && (3)\\
c_2 &= (c_1 b_1 - 1)/b_2 && (4)\\
x_1 &= y_1^{c_1}(y_2^{c_2})^{-1} \bmod n && (5)
\end{aligned}$$

The fourth equation tells us that

$$c_1 b_1 - c_2 b_2 = 1$$

Now plug the definitions of y_1 and y_2 into (5), which gives us

$$\begin{aligned}
x_1 &= x^{b_1 c_1}(x^{b_2 c_2})^{-1} \bmod n\\
&= x^{b_1 c_1 - b_2 c_2} \bmod n\\
&= x^1 \bmod n\\
&= x.
\end{aligned}$$

[**Note:** Since

$$\begin{aligned}
c_1 &= b_1^{-1} \bmod b_2\\
y_1 &= x^{b_1} \bmod n,
\end{aligned}$$

it is very tempting to conclude that

$$y_1^{c_1} \equiv (x^{b_1})^{b_1^{-1} \bmod b_2} \equiv x^1 \equiv x \pmod{n}.$$

However, the exponent for the second term here is $b_1 \cdot (b_1^{-1} \bmod b_2)$; and this is not the same as $(b_1 \cdot b_1^{-1}) \bmod b_2$. For example, $2^{-1} \bmod 5 = 3$. Therefore,

$$2 \cdot (2^{-1} \bmod 5) = 2 \cdot 3 = 6.$$

It would be OK if the exponent looked like this: $(b_1 \cdot (b_1^{-1} \bmod b_2)) \bmod b_2$. But this isn't what we have.]

4. Recall our discussion of partial information on RSA. We defined the functions,

$$
\begin{aligned}
parity(x^e \bmod n) &= \begin{cases} 0 & \text{if } x \bmod n \text{ is even} \\ 1 & \text{if } x \bmod n \text{ is odd} \end{cases} \\
half(x^e \bmod n) &= \begin{cases} 0 & \text{if } x \bmod n < n/2 \\ 1 & \text{if } x \bmod n > n/2 \end{cases}
\end{aligned}
$$

Here e and n are the usual RSA public key parameters. x is an RSA plaintext message, which means that it's an integer less than n.

Prove the following:

$$\text{if } half(x^e \bmod n) = 1, \text{ then } parity((2x)^e \bmod n) = 1.$$

Proof

We're given that $half(x^e \bmod n) = 1$. By definition of $half$, $x \bmod n > n/2$. Combining this with the fact that $x < n$ gives us that $n < 2x < 2n$. Therefore, $2x \bmod n = 2x - n$. Since $2x$ is even and n is odd, it follows that $2x \bmod n$ is odd. And this means, by the definition of $parity$, that $parity((2x)^e \bmod n = 1$.

6. Suppose that p is prime, $r > 0$, $a^r \equiv 1 \bmod p$, and $gcd(r, p-1) = d$. Prove that $a^d \equiv 1 \bmod p$.

Proof Since $gcd(r, p-1) = d$, there exist integers x and y such that $d = rx + (p-1)y$. Therefore,

$$
\begin{aligned}
a^d &\equiv a^{rx+(p-1)y} \\
&\equiv a^{rx}a^{(p-1)y} \\
&\equiv a^{(p-1)y} \bmod p \quad (\text{since } a^r \equiv 1 \bmod p)
\end{aligned}
$$

We'd like now to apply the FLT to $a^{(p-1)y} \bmod p$. But in order to justify applying the FLT here, we have to establish that p does not divide a. This *almost* follows just from the assumption that $a^r \equiv 1 \bmod p$: we'd like to say that if p did divide a, then $a^r \bmod p$ would be 0. However, this isn't quite right, since if r were 0, then $a^r \equiv 1 \bmod p$ even if p does divide a. This is why we need the assumption that $r > 0$; this assumption, together with the assumption that $a^r \equiv 1 \bmod p$, does imply that p does not divide a.

Therefore, we can apply the FLT to the last line of the above calculation to obtain

$$\begin{aligned} a^d &\equiv a^{(p-1)y} \bmod p \\ &\equiv 1 \pmod p \quad (\text{since } a^{p-1} \equiv 1 \bmod p, \text{ by the FLT}) \end{aligned}$$

7. Prove that if p is prime and $x^2 \equiv 1 \bmod p$, then

$$x \equiv 1 \bmod p \quad \text{or} \quad x \equiv -1 \bmod p.$$

Proof By basic fact (i), $x^2 \equiv 1 \bmod p$ implies that

$$p|(x^2 - 1).$$

In other words,

$$p|(x-1)(x+1).$$

Therefore, it follows by Theorem 2.2 in the number theory notes that $p|(x-1)$ or $p|(x+1)$ (if a prime divides a product, it must divide one of the terms in that product). In the first case, it follows from basic fact (i) that

$$x \equiv 1 \bmod p;$$

in the second case, it follows from basic fact (i) that

$$x \equiv -1 \bmod p.$$

8. Prove that if $x \equiv y \bmod \phi(m)$, then for any $a \in Z_m^*$, $a^x \equiv a^y \pmod m$.

Proof By basic fact (i),

$$\phi(m)|(x-y).$$

Therefore, for some k, $x = y + k \cdot \phi(m)$. So we have

$$\begin{aligned} a^x &\equiv a^{y+k\cdot\phi(m)} \\ &\equiv a^y \cdot a^{k\cdot\phi(m)} \\ &\equiv a^y \cdot 1 \quad \text{by Euler's Theorem} \\ &\equiv a^y \bmod m \end{aligned}$$