Math 116 HW5 Jun Ryu

1) a) $N = 1739$, $a = 2$

$n=1$ $2^{1!} - 1 \equiv 1$ $\gcd(1, 1739) = 1$

$n=2$ $2^{2!} - 1 \equiv 3$ $\gcd(3, 1739) = 1$

$n=3$ $2^{3!} - 1 \equiv 63$ $\gcd(63, 1739) = 1$

$n=4$ $2^{4!} - 1 \equiv 1082$ $\gcd(1082, 1739) \equiv 1$

$n=5$ $2^{5!} - 1 \equiv 1394$ $\gcd(1394, 1739) \equiv 1$

$n=6$ $2^{6!} - 1 \equiv 1443$ $\gcd(1443, 1739) = 37$

So, we get $1739 = \boxed{37 \cdot 47}$

$p - 1 = 36 = 2^2 \cdot 3^2$
$q - 1 = 46 = 2 \cdot 23$
$\Rightarrow$ $p-1$ is a product of small primes

b) $N = 220459$, $a = 2$

For $n = 1, 2, 3$, we check that $\gcd(1, 220459)$, $\gcd(3, 220459)$, and $\gcd(63, 220459)$ are all equal to 1.

$n=4$ $2^{4!} - 1 \equiv 22331$ $\gcd(22331, 220459) = 1$

$n=5$ $2^{5!} - 1 \equiv 85053$ $\gcd(85053, 220459) = 1$

$n=6 \quad 2^{6!}-1 \equiv 4045 \quad \gcd(4045, 220459) = 1$

$n=7 \quad 2^{7!}-1 \equiv 43102 \quad \gcd(43102, 220459) = 1$

$n=8 \quad 2^{8!}-1 \equiv 179600 \quad \gcd(179600, 220459) = 449$

So, we get $220459 = \boxed{449 \cdot 491}$

$p-1 = 448 = 2^6 \cdot 7$

$q-1 = 490 = 2 \cdot 5 \cdot 7^2$

$\Rightarrow$ $p-1$ is a product of small primes

2) a)

integers from 2 to 25 that are 3-smooth:

2, 3, 4, 6, 8, 9, 12, 16, 18, 24

So, $\Psi(25,3) = \boxed{10}$

b) integers from 2 to 35 that are 5-smooth:

2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 32

So, $\Psi(35,5) = \boxed{18}$

c) integers from 2 to 50 that are NOT 7-smooth:

11, 13, 17, 19, 22, 23, 26, 29, 31, 33, 34, 37, 38, 39, 41, 43, 44, 46, 47

So, $\Psi(50,7) = 49 - 19 = \boxed{30}$

3) Since $192 = 2^6 \cdot 3$ and $15552 = 2^6 \cdot 3^5$,

we try $763^2 \cdot 773^2 \equiv 192 \cdot 15552 \pmod{52907}$

$$\equiv (2^6 \cdot 3)(2^6 \cdot 3^5) \equiv (2^6 \cdot 3^3)^2 = 1728^2$$

So, $\boxed{a = 763 \cdot 773 \text{ and } b = 1728}$

where $a^2 \equiv b^2 \pmod{N}$

Now, $\gcd(52907, 763 \cdot 773 - 1728)$

$= \boxed{277}$

4) a) Let $a^{(p-1)/2} = x$. Then, we have

$$x^2 = (a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem.

So, we have $x^2 - 1 \equiv 0 \pmod{p}$

$= (x+1)(x-1) \equiv 0 \pmod{p}$

So, $p \mid (x+1)(x-1)$ and p is prime

$\Rightarrow$ $x \equiv 1$ or $-1 \pmod p$ ✓

b) ($\Leftarrow$) Let a be a quad. residue modulo p.

Let g be a primitive root for p.

Then, g^m is a quadratic residue iff

m is even. So, let $m = 2k$ and set $g^{2k} = a$

calculate $(g^{2k})^{(p-1)/2} \equiv g^{k(p-1)}$

$\equiv (g^{p-1})^k \equiv 1^k = 1 \pmod p$ ✓

($\Rightarrow$) Let $a^{(p-1)/2} \equiv 1 \pmod p$

Let $a \equiv c^2 \pmod p$, then

$(c^2)^{(p-1)/2} \equiv c^{p-1} \equiv 1 \pmod p$.

Thus, such a c exists, and by the def. of quad. residue, a is a quadratic residue mod p. ✓

5) We compute $\left(\frac{35}{101}\right)$

$$\left(\frac{35}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{7}{101}\right)$$

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

So, $\left(\frac{5}{101}\right)\left(\frac{7}{101}\right) = \left(\frac{101}{5}\right)\left(\frac{101}{7}\right)$

$$= \left(\frac{1}{5}\right)\left(\frac{3}{7}\right) = -\left(\frac{1}{5}\right)\left(\frac{7}{3}\right) = -\left(\frac{1}{5}\right)\left(\frac{1}{3}\right)$$

Since 1 is a quad. residue modulo 3 and 5 ($2^2 \equiv 1 \pmod 3$, $4^2 \equiv 1 \pmod 5$),

$$-\left(\frac{1}{5}\right)\left(\frac{1}{3}\right) = \boxed{-1}$$

6) a) We decrypt by computing $\left(\frac{c}{p}\right)$, where $m = \begin{cases} 0 & \text{if } \left(\frac{c}{p}\right) = 1 \\ 1 & \text{if } \left(\frac{c}{p}\right) = -1 \end{cases}$

So, first, we do $\left(\frac{1794677960}{32411}\right) = -1$

$\Rightarrow m=1$

Then, we do $\left(\frac{525734818}{32411}\right) = 1 \Rightarrow m=0$

Lastly, $\left(\frac{420526487}{32411}\right) = -1 \Rightarrow m=1$

So, the plaintext is $\boxed{(1,0,1)}$

b) We encrypt $m=1$ by calculating

$c_1 \equiv a r_1^2 \pmod N$.

$c_1 \equiv 568980706 \cdot 705130839^2 \equiv \boxed{517254876} \pmod{781044643}$

$c_2 \equiv 568980706 \cdot 631364468^2 \equiv \boxed{4308279} \pmod{781044643}$

Encrypt $m=0$ by calculating $c_3 \equiv r_3^2 \pmod N$

$c_3 \equiv 67651321^2 \equiv \boxed{660699010} \pmod{781044643}$

7) a)

Samantha's public modulus is

$N = 541 \cdot 1223 = \boxed{661643}$

We solve for her private signing key by solving $ed \equiv 1 \pmod{(p-1)(q-1)}$

So, $159853d \equiv 1 \pmod{659880}$,

which gives us $d = \boxed{561517}$

b) We can get her signature by solving

$S \equiv D^d \pmod{N}$

So, $S \equiv 630579^{561517} \pmod{661643}$,

giving us $S = \boxed{206484}$

8) We can verify signatures by checking

$D \stackrel{?}{\equiv} S^e \pmod{N}$

So, $S^e \equiv 876453^{87953} \equiv 772481 \pmod{1562501}$

$\neq 119812 = D$

$$(s')^e \equiv 870099^{87953} \equiv 161153 = D' \pmod{1562501}$$

$$(s'')^e \equiv 602754^{87953} \equiv 586036 = D'' \pmod{1562501}$$

So, S is not a valid signature, while s' and s'' are