1 SPCS

1.1

2 Chinese Remainder Theorem

Find numbers that satisfy the following congruences:

2.1

- $x \equiv 2 \pmod{5}$
- $x \equiv 1 \pmod{7}$

[SOLUTION: 22]

2.2

- $x \equiv 9 \pmod{13}$
- $x \equiv 4 \pmod{24}$

[SOLUTION: 100]

2.3

- $x \equiv 1 \pmod{2}$
- $x \equiv 1 \pmod{3}$
- $x \equiv 2 \pmod{5}$

[SOLUTION: 7]

2.4

- $x \equiv 4 \pmod{7}$
- $x \equiv 3 \pmod{11}$
- $x \equiv 8 \pmod{13}$

[SOLUTION: 333]

3 Chinese Remainder Theorem with Friends

Pick a partner you haven't worked with before.

Ask them to select a number x from 1 to 60 and tell you:

- $x \pmod 3$
- $x \pmod 4$
- $x \pmod 5$

Now, calculate x (if you get something outside of the range $1, ..., 60$, remember that you can add ay multiple of 60 and the congruences remain valid).

4 Speeding up RSA

Do an RSA encryption with a partner as in previous homeworks. However, when you decrypt, calculate:

- $c^d \mod p$
- $c^d \mod q$

Now, use these values to calculate $c^d \mod N$ using the Chinese Remainder Theorem.

5 Factoring

5.1

Factor the following numbers using trial division (you can use a calculator, but don't use a function that factors numbers for you):

- 34111
- 11121
- 1001
- 483

Make sure every factor you end up with is prime.

5.2

Use the difference of two squares to factor the following numbers:

- 323 [SOLUTION: (18+1)(18-1)]
- 105 [SOLUTION: (13+8)(13-8)]
- 221 [SOLUTION: (13+8)(13-8)]
- 8099 [SOLUTION: (93+4)(93-4)]

5.3

Use the Fermat primality test to find witnesses and prove numbers from the previous section composite.

6 RSA Blind Signatures

6.1

Let's show that it's possible to sign a message using RSA without knowing what the message is.

Suppose Bob has a private key (N, e) for the RSA signature scheme, and Alice wants him to sign m. Alice does the following:

- Select a random $r \in \mathbb{Z}_N^*$.
- Calculate $r' = r^d$ This is the *blinding value*.
- Blind m using r' to by multiplying: $m' = m \cdot r'$.
- Ask Bob to sign m' to get $s' = Sign(sk, m')$.
- (Convert s' into a valid signature of s.)

Calculate the value of s' in terms of m, r, and the RSA parameters (N, e, d). Use this to figure out sweat should go in the last step. That is, how Alice can use s' to get a valid signature s that will pass verification:

$$\text{Verify}(pk, s, m) = \left(m \stackrel{?}{=} s^d \bmod N\right)$$

Explain why it is impossible for Bob to find out what message m he was signing if he doesn't know r or r'.

In particular, can you show that it is *completely* impossible for Bob to get any information about m? (Except that $m \in \mathbb{Z}_n$, which he already knows.)

6.2

Try this operation with a partner.

6.3

Is this cool or what?