1. (§2.4, problem 9) Show that if $x^2 \equiv 1 \pmod{m}$ and $x \not\equiv \pm 1 \pmod{m}$ then

$$1 < (x-1, m) < m \quad \text{and} \quad 1 < (x+1, m) < m.$$

Proof: From $x^2 \equiv 1 \pmod{m}$ we get

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

We factor $x^2 - 1$ to get

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

We are given $x \not\equiv 1 \pmod{m}$ and $x \not\equiv -1 \pmod{m}$. This implies that $m \not| x-1$ and $m \not| x+1$. From these, we can conclude immediately that

$$(x-1, m) < m \quad \text{and} \quad (x+1, m) < m.$$

Moreover, if $(x-1, m) = 1$, then from $m|(x-1)(x+1)$ and Theorem 1.10, we conclude that $m|x+1$, contrary to hypothesis. Thus $(x-1, m) > 1$.

Similarly, if $(x+1, m) = 1$, then since $m|(x-1)(x+1)$, we can conclude that $m|x-1$, contrary to hypothesis. Thus $(x+1, m) > 1$.

2. Remember to write in complete sentences.

(a) (§2.4, problem 2) Use the calculator to verify that $2^{45} \equiv 57 \pmod{91}$. Explain why this proves that 91 is composite.

Solution: According to the calculator, 2^{45} is indeed congruent to 57 modulo 91. If 91 were prime, we'd have $2^{90} \equiv 1 \pmod{91}$, and since $(2^{45})^2 = 2^{90} \equiv 1 \pmod{91}$, we'd also have (by Lemma 2.10)

$$2^{45} \equiv \pm 1 \pmod{91}.$$

Since $2^{45} \equiv 57 \not\equiv \pm 1 \pmod{91}$, we can conclude that 91 is not prime.

(b) (§2.4, problems 5 and 6) Show that 2047 is a strong probable prime to the base 2, but not to the base 3.

Solution: We note that $2046 = 2 \times 1023$. Using the calculator, we deterime that

$$2^{2046} \equiv 1 \pmod{2047}$$

and

$$2^{1023} \equiv 1 \pmod{2047}.$$

The first fact shows that 2047 is a probable prime to the base 2. The second fact shows that 2047 is a strong probable prime to the base 2, because 1023 is odd, so we can't take any more square roots.

To show that 2047 is not a strong probably prime to the base 3, we use a calculator to find that

$$3^{2046} \equiv 1013 \pmod{2047}.$$

Since $1013 \not\equiv 1 \pmod{2047}$, we can conclude that 2047 is not even a probable prime to the base 3, much less a strong probable prime.

So we know 2047 is in fact composite.

3. (a) Universal Exports spymaster M wants her field agent, Jimmy, to send her a highly sensitive, top-secret telephone number via email. She decides to use public-key cryptography, and sends Jimmy the encoding keys $m = 8228747$ and $k = 24919$. Jimmy dutifully encrypts the secret phone number, and emails the result, 4100849, back to M.

Members of SPECTRUM, an idealistic group opposed to any kind of spying whatsoever, intercept the whole transaction, and discover that M has made a terrible mistake. The number 8228747 is prime! Using this information, they quickly discover the crucial phone number. What is it?

Solution: Since m is prime, $\varphi(m) = m - 1$, so by use of the Euclidean algorithm, we can easily find $\overline{k}$ modulo $m - 1$.

I wrote a little TI-85 program to do this; it tells me that

$$11290 \times 8228746 - 3728181 \times 24919 = 1$$

so that $\overline{k} \equiv -3728181 \equiv 4500565 \pmod{8228746}$. Using this decrypting $\overline{k}$ and another TI-85 program, I get

$$4100849^{4500565} \equiv 5682267 \pmod{8228747}.$$

This turns out to be the phone number of the automated weather observation station at the Westfield Barnes airport.

(b) Not one to repeat her mistakes, the next day M sends Jimmy the encryption keys $m = 8228743$ (which is composite) and $k = 1237$, and asks him to send back the number of solutions he found to $\varphi(x) = 48$, the study of which is an important government project. Jimmy's encrypted response is 5166026.

SPECTRUM members once again monitor the whole exchange and manage to decrypt Jimmy's answer, but only because (1) they have access to a sophisticated hand calculator or personal computer and (2) M's m is too small to be secure. What do they do, and what answer do they get?

Solution: They somehow manage to factor 8228743. Several computer algebra systems will do this – the smallest device I found that could factor this number is a TI-89. It says

$$8228743 = 2411 \times 3413.$$

Both these factors are prime, so $\varphi(8228743) = \varphi(2411)\varphi(3413) = 2410 \times 3412 = 8222920$.

As before, we need to invert k modulo $\varphi(m)$. My calculator program gives

$$438733 \times 1237 - 66 \times 8222920 = 1$$

so that we may take $\overline{k} = 438733$.

Using the calculator once again to decrypt Jimmy's answer, we get

$$5166026^{438733} \equiv 11 \pmod{8228743}.$$

(c) Jimmy begins to have doubts about some of the instructions he's receiving from M. Assuming that M is the only person in the world who knows how to factor the number $m = 8228743$, what can Jimmy and M do (without compromising the security of m or M) to verify that Jimmy's orders are coming from M and not from some imposter?

Solution: Jimmy asks for an encryption key k, which M supplies. He then randomly selects a number a relatively prime to m and sends that number to M. M knows $\varphi(m)$, so she can easily find the number $\overline{k}$ such that $k\overline{k} \equiv 1 \pmod{\varphi(m)}$. She sends Jimmy the number $a^{\overline{k}}$. Jimmy raises this to the power k, reducing modulo m. If he gets back his original number a, then he knows he's talking to M.

4. Note that Lemma 2.22 requires that the number a (the "message") be relatively prime to m. Thus it appears that RSA encryption will fail for certain messages.

(a) Suppose $m = pq$, where p and q are primes. We select an integer a at random from the set $\mathcal{S} = \{0, 1, 2, \ldots, m-1\}$. Find

$$P((a, m) > 1)$$

that is, the probability that $(a, m) > 1$. (Give your answer in terms of p and q.)

If p and q are both primes on the order of 10^{100}, what is the order of magnitude of $P((a, m) > 1)$?

Solution: There are m numbers in $\mathcal{S}$, of which q numbers are divisble by p and p numbers are divisible by q. Only one number (zero) is divisible by both p and q, so the number of elements a of $\mathcal{S}$ satisfying $(a, m) > 1$ is $p+q-1$. The probability of selecting one of these numbers at random is

$$\frac{p+q-1}{m} = \frac{p+q-1}{pq}.$$

If p and q are on the order of 10^{100}, then so is $p+q-1$. The number $m = pq$, on the other hand, will be on the order of 10^{200}, so we get

$$P((a, m) > 1) \approx 10^{-100}.$$

This is approximately the probability of tossing a fair coin 332 times and having it come up heads every time.

(b) (§2.5, problem 4) In fact, as long as m is square-free, it turns out that RSA encryption and decryption will work for any value of a, whether or not it's relatively prime to m. Prove the following:

Suppose $m = p_1 p_2 \cdots p_r$ is a product of the distinct primes $p_1, p_2, \ldots, p_r$. Suppose that k and $\overline{k}$ are positive integers such that

$$k\overline{k} \equiv 1 \pmod{\varphi(m)}.$$

Then $a^{k\overline{k}} \equiv a \pmod{m}$ for all integers a.

Solution: Suppose m, k, and $\overline{k}$ are as given in the theorem.

Claim: If $p_i \nmid a$, then $a^{k\overline{k}} \equiv a \pmod{p_i}$.

Proof of claim: First we note that $\varphi(p_i) = p_i - 1$ and that

$$\varphi(m) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1)$$

so that $\varphi(p_i)|\varphi(m)$. Thus by Theorem 2.1(5), we get $k\overline{k} \equiv 1 \pmod{\varphi(p_i)}$. Since $p_i \not| a$ and p_i is prime, we have $(a, p_i) = 1$, so by Lemma 2.22, we conclude that

$$a^{k\overline{k}} \equiv a \pmod{p_i}.$$

Claim: If $p_i|a$, then $a^{k\overline{k}} \equiv a \pmod{p_i}$.
Proof of claim: In this case, $a \equiv 0 \pmod{p_i}$, so that

$$a^{k\overline{k}} \equiv 0^{k\overline{k}} \equiv 0 \pmod{p_i}.$$

Then by transitivity (Theorem 2.1(2)), we get

$$a^{k\overline{k}} \equiv a \pmod{p_i}.$$

Proof of theorem: Let a be any integer. For each $i = 1, \ldots, r$, either $p_i|a$ or $p_i \not| a$. In either case, we can conclude from one of the two claims above that

$$a^{k\overline{k}} \equiv a \pmod{p_i}.$$

By Theorem 2.3(3), we get

$$a^{k\overline{k}} \equiv a \pmod{[p_1, p_2, \ldots, p_r]},$$

and since the p_i are all distinct primes, we know they are relatively prime (in pairs), so that

$$[p_1, p_2, \ldots, p_r] = p_1 p_2 \cdots p_r = m.$$

Thus we get

$$a^{k\overline{k}} \equiv a \pmod{m}$$

for any integer a. ∎

(c) The hypothesis that m be square-free in part (4b) is necessary. Find an example of a modulus m, an integer a, and two positive integers k and $\overline{k}$ with

$$k\overline{k} \equiv 1 \pmod{\varphi(m)}$$

such that $a^{k\overline{k}} \not\equiv a \pmod{m}$.

Explain how you found your example.

Solution: Take $m = 9$, $a = 6$, and $k = \overline{k} = 5$. We have

$$\varphi(9) = 9 - 3 = 6$$

and $k\overline{k} = 25 \equiv 1 \pmod 6$, so that k and $\overline{k}$ satisfy the conditions above. However, we know that $3|6$, so the number

$$a^{k\overline{k}} = 6^{25}$$

is divisible by 3^{25}, and in particular, it's divisible by 9. Thus we have

$$a^{k\overline{k}} = 6^{25} \equiv 0 \pmod 9.$$

Since $6 \not\equiv 0 \pmod 9$, we have an example wherein

$$a^{k\overline{k}} \not\equiv a \pmod m.$$

To find this example, I chose $m = 9$, a small modulus that is *not* square-free. Since $\varphi(9) = 6$, the only non-trivial choice for k was 5. I made up a table of fifth powers modulo 9, and noticed that $6^5 \equiv 0 \pmod 9$.

Since no power of 0 can be congruent to 6 modulo 9, this is an example of the phenomenon we're looking for.