Math 319 Problem Set #7 Due 18 April 2002

Reading: NZM §§2.4, 2.5

Exercises: Write your solutions in complete sentences.

For the numerical computations in this problem set, you may use either a hand calculator or the calculation routines provided on the course website (from the "Resources" page). You don't have to write out every step – we will assume that powermod and GCD calculations are easy.

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

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

HINT: Use Theorem 1.10.

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.

(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.

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?

(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?

(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?

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

(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.

HINT: First prove two lemmata (using the notation of the theorem):

(1) If $p_i \nmid a$ then $a^{k\overline{k}} \equiv a \pmod{p_i}$;
(2) If $p_i | a$ then $a^{k\overline{k}} \equiv a \pmod{p_i}$.

(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.

Cultural aside:

"You're wasting your time," Doc Daneeka was forced to tell him.

"Can't you ground someone who's crazy?"

"Oh, sure. I have to. There's a rule saying I have to ground anyone who's crazy."

"Then why don't you ground me? I'm crazy. Ask Clevinger."

"Clevinger? Where *is* Clevinger? You find Clevinger and I'll ask him."

"Then ask any of the others. They'll tell you how crazy I am."

"They're crazy."

"Then why don't you ground them?"

"Why don't they ask me to ground them?"

"Because they're crazy, that's why."

"Of course they're crazy," Doc Daneeka replied. "I just told you they're crazy, didn't I? And you can't let crazy people decide whether you're crazy or not, can you?"

Yossarian looked at him soberly and tried another approach. "Is Orr crazy?"

"He sure is," Doc Daneeka said.

"Can you ground him?"

"I sure can. But first he has to ask me to. That's part of the rule."

"Then why doesn't he ask you to?"

"Because he's crazy," Doc Daneeka said. "He has to be crazy to keep flying combat missions after all the close calls he's had. Sure, I can ground Orr. But first he has to ask me to."

"That's all he has to do to be grounded?"

"That's all. Let him ask me."

"And then you can ground him?" Yossarian asked.

"No. Then I can't ground him."

"You mean there's a catch?"

"Sure there's a catch," Doc Daneeka replied. "Catch-22. Anyone who wants to get out of combat duty isn't really crazy."

There was only one catch and that was Catch-22, which specified that a concern for one's own safety in the face of dangers that were real and immediate was the process of a rational mind. Orr was crazy and could be grounded. All he had to do was ask; and as soon as he did, he would no longer be crazy and would have to fly more missions. Orr would be crazy to fly more missions and sane if he didn't but if he was sane he had to fly them. If he flew them he was crazy and didn't have to; but if he didn't want to he was sane and had to. Yossarian was moved very deeply by the absolute simplicity of this clause of Catch-22 and let out a respectful whistle.

"That's some catch, that Catch-22," he observed.

"It's the best there is," Doc Daneeka agreed.

Joseph Heller, *Catch-22*