Math 319 Problem Set #4 Due 12 March 2000

Reading: NZM §§2.1, 2.2.

Exercises: Write your solutions in complete sentences.

1. (§2.1, problem 34) Show that an integer $m > 1$ is a prime if and only if m divides $(m-1)! + 1$.

2. (§1.2, problem 32) Let $n \geq 2$ and k be any positive integers. Prove that $(n-1)^2 | (n^k - 1)$ if and only if $(n-1)|k$.

3. (Based on §2.1, problem 43) Let p be an odd prime. Show that $\{2, 4, 6, \ldots, 2(p-1)\}$ is a reduced residue system modulo p. Use this result to show that if p is an odd prime, then

$$2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

4. (§2.1, problem 54)

(a) Note that $341 = 11 \cdot 31$. Without using excessive computer power, show that $2^{341} \equiv 2 \pmod{341}$, but that $3^{341} \not\equiv 3 \pmod{341}$.

(Because of the first fact above, the number 341 is called a *pseudoprime to the base* 2. The second fact shows that 341 is not actually prime; the number 3 is called a *witness* to the compositeness of 341.)

(b) Show that 561 is a pseudoprime to every base, even though 561 is not prime.

(The number 561, which is composite ($561 = 3 \cdot 11 \cdot 17$) but admits no witnesses to its compositeness, is called a *Carmichael number*.)

Cultural aside:

[Holmes] saw the question in my eyes, and, putting his finger-tips together and his elbows upon his knees, he explained the situation.

"You have probably never heard of Prefessor Moriarty?" said he.

"Never."

"Ay, there's the genius and the wonder of the thing!" he cried. "The man pervades London, and no one has heard of him. That's what puts him on a pinnacle in the records of crime. I tell you Watson, in all seriousness, that if I could beat that man, if I could free society of him, I should feel that my own career had reached its summit, and I should be prepared to turn to some more placid line in life. ... But I could not rest, Watson, I could not sit quiet in my chair, if I thought that such a man as Professor Moriarty were walking the streets of London unchallenged.

"What has he done, then?"

"His career has been an extraordinary one. He is a man of good birth and excellent education, endowed by nature with a phenomenal mathematical faculty. At the age of twenty-one he wrote a treatise upon the binomial theorem, which has had a European vogue. On the strength of it he won the mathematical chair at one of our smaller universities, and had, to all appearances, a most brilliant career before him. But the man had hereditary tendencies of the most diabolical kind. A criminal strain ran in his blood, which, instead of being modified, was increased and rendered infinitely more dangerous by his extraoridnary mental powers. Dark rumors gathered round him in the university town, and eventually he was compelled to resign his chair and to come down to London, where he set up as an army coach. So much is known to the world, but what I am telling you now is what I have myself discovered.

...

"He is the Napoleon of crime, Watson. He is the organizer of half that is evil and of nearly all that is undetected in this great city. He is a genius, a philosopher, an abstract thinker. He has a brain of the first order. He sits motionless, like a spider in the centre of its web, but that web has a thousand radiations, and he knows well every quiver of each of them. He does little himself. He only plans. But his agents are numerous and splendidly organized. Is there a crime to be done, ... the word is passed to the professor, the matter is organized and carried out."

Sir Arthur Conan Doyle, *Memoirs of Sherlock Holmes*