MA2316: Introduction to Number Theory
Tutorial problems for February 6, 2014

"Modular arithmetic"

1. Show that the map $\tau\colon \mathbb{Z}/(ab)\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ defined as $\tau(n+ab\mathbb{Z}) = (n+a\mathbb{Z}, n+b\mathbb{Z})$ is a ring homomorphism. Use the First Isomorophism Theorem to show that for coprime a and b it is a ring isomorphism. (This statement about isomorphism is sometimes called the Chinese Remainder Theorem; the next problem will construct the inverse of τ which is was an important accomplishment of Chinese mathematics around the 5th century).

2. Suppose a and b are coprime. Use integer solutions to $ax + by = 1$ to solve the systems of simultaneous congruences

$$\begin{cases} x \equiv 1 \pmod{a}, \\ x \equiv 0 \pmod{b} \end{cases}$$

and

$$\begin{cases} x \equiv 0 \pmod{a}, \\ x \equiv 1 \pmod{b}. \end{cases}$$

Show that in general for all m and n the system of simultaneous congruences

$$\begin{cases} x \equiv m \pmod{a}, \\ x \equiv n \pmod{b} \end{cases}$$

has solutions, and its solution is unique modulo ab.

3. Solve the system of congruences

$$\begin{aligned} x &\equiv 11 \pmod{23}, \\ x &\equiv 12 \pmod{25}, \\ x &\equiv 13 \pmod{27}. \end{aligned}$$

4. For which a does the following system of congruences have integer solutions? (*Hint*: $100 = 25 \cdot 4$, $35 = 5 \cdot 7$).

$$\begin{aligned} x &\equiv a \pmod{100}, \\ x &\equiv b \pmod{35}. \end{aligned}$$

5. Show that there are infinitely many prime numbers q such that $2q + 1$ is not a prime. (*Hint*: Fermat's Little Theorem might be helpful at some point.)

6. In class, it will be shortly proved that for an odd prime p the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has solutions if and only if $p \equiv 1 \pmod{4}$. Using that, show that for every n all prime divisors of $4n^2 + 1$ are of the form $4k + 1$, and adapt the Euclid's "$p_1p_2\cdots p_n - 1$"-argument proving the infinitude of primes to show that there are infinitely many primes of the form $4k+1$.