MATH 255: ELEMENTARY NUMBER THEORY
HOMEWORK #6

JOHN VOIGHT

p-adic Numbers

Problem A*. Let p be prime. For $0 \neq x \in \mathbb{Z}$, let $\mathrm{ord}_p(x)$ denote the power of p that exactly divides x, i.e., $\mathrm{ord}_p(x) = e$ if and only if $p^e \parallel x$. Let $\mathrm{ord}_p(0) = \infty$.

(a) Show that $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$ for all $x, y \in \mathbb{Z}$.
(b) Show that $\mathrm{ord}_p(x+y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$ for all $x, y \in \mathbb{Z}$.

Now define $|x|_p = p^{-\mathrm{ord}_p(x)}$ if $x \neq 0$ and $|0|_p = 0$.

(c) Show that $|xy|_p = |x|_p|y|_p$ and prove the *triangle inequality*

$$|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$$

for all $x, y \in \mathbb{Z}$. In particular, this shows that $|\,|_p$ gives an absolute value on $\mathbb{Z}$.
(d) Given $x, y \in \mathbb{Z}$, we define the *distance* $d_p(x,y) = |x-y|_p$. When $p = 2$, is $x = 17$ or $x = 3$ closer to $y = 1$?

6.1: Wilson's Theorem and Fermat's Little Theorem

Problem 6.1.3. What is the remainder when 16! is divided by 19?

Problem 6.1.12. Using Fermat's little theorem, find the least positive residue of $2^{1000000}$ modulo 17.

Problem 6.1.25. Show that if p is prime and a and b are integers not divisible by p, with $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

Problem 6.1.28. Show that if p and q are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Problem 6.1.36*. For which positive integers n is $n^4 + 4^n$ prime?

Problem 6.1.43. A deck of cards is shuffled by cutting the deck into two piles of 26 cards. Then, the new deck is formed by alternating cards from the two piles, starting with the bottom pile.

(a) Show that if a card begins in the cth position in the deck, it will be in the bth position in the new deck, where $b \equiv 2c \pmod{53}$ and $1 \leq b \leq 52$.
(b) Determine the number of shuffles of the type described above that are needed to return the deck of cards to its original order.

Date: Due Wednesday, 4 March 2009.

6.3: Euler's Theorem

Problem 6.3.A. Find a reduced residue system modulo 7 consisting only of powers of 3.

Problem 6.3.9. Show that if $a \in (\mathbb{Z}/32760\mathbb{Z})^*$ then $a^{12} \equiv 1 \pmod{32760}$. Does this contradict Euler's theorem?

Group Theory

Problem A*. Show that there are only two groups G_1, G_2 of order 4 up to isomorphism, and that both G_1 and G_2 are abelian. Find (all) integers $m_1, m_2 \in \mathbb{Z}_{>0}$ such that $(\mathbb{Z}/m_1\mathbb{Z})^* \cong G_1$ and $(\mathbb{Z}/m_2\mathbb{Z})^* \cong G_2$.