Homework 7, due on Friday, March 13

Read carefully sections 5.3, 5.4 in the book. Solve problems 25d), 28a), 32c), 35, 38 and the following problems.

Problem 1. Let p be an odd prime number. Let a, b be integers such that $a \equiv b \pmod{p}$ and $\gcd(a,p) = 1$. Prove that

$$a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} \equiv p \pmod{p^2} .$$

Problem 2. Let p be an odd prime and let a, b be integers not divisible by p. In this problem we study the highest power of p which divides $a^n - b^n$ for positive integers n. Let m be the smallest positive integer such that $p|(a^m - b^m)$ and let p^s be the highest power of p which divides $a^m - b^m$ (so $s = e_p(a^m - b^m)$).

a) Let c be the inverse of b modulo p, so $bc \equiv 1 \pmod{p}$. Prove that $m = \mathrm{ord}_p(ac)$.

b) Prove that if $m \nmid n$ then $p \nmid a^n - b^n$.

From now on suppose that $m|n$. Thus we can factor $n = mp^kN$ for some $k \geq 0$ and some N not divisible by p.

c) Show that p^s is the highest power of p which divides $a^{mN} - b^{mN}$ (i.e. $e_p(a^{mN} - b^{mN}) = s$).

d) Use Problem 1 and induction on r to show that p^{s+r} is the highest power of p which divides $a^{mNp^r} - b^{mNp^r}$. Conclude that

$$e_p(a^n - b^n) = \begin{cases} 0 & \text{if } m \nmid n \\ e_p(a^m - b^m) + e_p(n) & \text{if } m|n. \end{cases}$$

e) Find and prove a similar formula for $e_2(a^n - b^n)$ for odd integers a, b.

Problem 3. Let p, q, r be three distinct prime numbers. Prove that

$$(pq)^{r-1} + (pr)^{q-1} + (qr)^{p-1} \equiv 1 \pmod{pqr} .$$

Problem 4. Let m, n be positive integers such that $m|n$. Prove that $\phi(m)|\phi(n)$ and $\phi(mn) = m\phi(n)$.

Problem 5. Let m, n be relatively prime positive integers and let a be relatively prime to mn. Prove that $\mathrm{ord}_{mn}a = \mathrm{lcm}(\mathrm{ord}_m a, \mathrm{ord}_n a)$.

Problem 6. Let $p < q$ be odd prime numbers. Prove that pq is not a Carmichael number. Hint: Show first that there is an integer a which is a primitive root modulo p and a primitive root modulo q (use Chinese Reminder Theorem).

Problem 7. Let a, b, c be integers. Prove that

$$\mathrm{lcm}(\gcd(a,b), \gcd(a,c)) = \gcd(a, \mathrm{lcm}(b,c))$$

and

$$\mathrm{lcm}(a,b,c) = \frac{abc\ \gcd(a,b,c)}{\gcd(a,b)\gcd(a,c)\gcd(b,c)}.$$

Hint: One approach is to verify this by evaluating e_p of each side for every prime p.

Problem 8. Find the decimal expansion of $\dfrac{102}{10175}$ without using calculator.