ELEMENTARY NUMBER THEORY

HOMEWORK 2

(1) Show that there are infinitely many primes of the form $p \equiv 3 \bmod 4$ by modifying Euclid's proof.

Assume that $p_1 = 3, \ldots, p_n$ are primes of the form $p_j \equiv 3 \bmod 4$. We will construct a new one by looking at $N = 4p_1 \cdots p_n - 1$ (putting $N = 4p_1 \cdots p_n + 3$ would also work). First, none of the primes p_j divides N: note that $p_j \mid N+1$, so if we had $p_j \mid N$, then we would have $p_j \mid (N+1) - N = 1$: contradiction. Now we observe that at least one of the prime factors of N has the form $p \equiv 3 \bmod 4$: in fact, N is odd, hence if such a prime does not exist, then all prime factors of N have the form $p \equiv 1 \bmod 4$; but then we would have $N \equiv 1 \bmod 4$ contradicting the construction of N.

Why does this trick not work for primes $p \equiv 1 \bmod 4$?

If we put $N = 4p_1 \cdots p_n + 1$, then $N \equiv 1 \bmod 4$, but we have no way of ensuring that N has some prime factor of the form $p \equiv 1 \bmod 4$. For example, starting with $p_1 = 5$ we get $N = 4 \cdot 5 + 1 = 21$, and $21 = 3 \cdot 7$.

Nevertheless it is possible to prove that there exist infinitely many primes of the form $p \equiv 1 \bmod 4$: all we have to do is put $N = 4(p_1 \cdots p_n)^2 + 1$. Then $p_j \nmid N$; moreover, if p is aprime factor of N, then $4(p_1 \cdots p_n)^2 \equiv -1 \bmod p$; but -1 is a quadratic residue modulo p if and only if $p \equiv 1 \bmod 4$. The rest of the proof goes through unchanged.

(2) Prove that
  (a) $\gcd(ma, mb) = m \cdot \gcd(a, b)$;
  (b) $\gcd(a, b) = \gcd(a, a + b)$.

(a) $\gcd(ma, mb) = m \cdot \gcd(a, b)$.
Let $d = \gcd(a, b)$; then $d \mid a$ and $d \mid b$, hence $md \mid ma$ and $md \mid mb$. This shows that $md \mid \gcd(ma, mb)$.
Now assume that $e \mid ma$ and $e \mid mb$. The Bezout representation of d is $d = ax + by$; this gives us $md = max + mby$, and since e divides the right hand side, we must have $e \mid md$.

(b) $\gcd(a, b) = \gcd(a, a + b)$.
If $d \mid a$ and $d \mid b$, then $d \mid a$ and $d \mid (a+b)$. Thus $\gcd(a, b) \mid \gcd(a, a+b)$.
On the other hand, if $d \mid a$ and $d \mid (a+b)$, then $d \mid a$ and $d \mid (a+b) - a = b$, hence $\gcd(a, a + b) \mid \gcd(a, b)$.
This shows that $\gcd(a, b) = \gcd(a, a + b)$.

(3) Show that if $n = x^2 + 2y^2$ is odd, then $n \equiv 1, 3 \bmod 8$.

If n is odd, then x must be odd, hence $x^2 \equiv 1 \bmod 8$. Moreover, $y^2 \equiv 0, 1, 4 \bmod 8$, hence $2y^2 \equiv 0, 2 \bmod 8$. This shows that $n = x^2 + 2y^2 \equiv 1, 3 \bmod 8$.

(4) Compute the last digit of 7^{100}.

The last digit of a number N can be determined by computing $N \bmod 10$. Now $7^2 = 49 \equiv -1 \bmod 10$, hence $7^4 \equiv 1 \bmod 10$ and finally $7^{100} = (7^4)^{25} \equiv 1^{25} \equiv 1 \bmod 10$. Thus the last digit of 7^{100} is 1.

A calculation with pari shows that $7^{100} = 32344 \ldots 060001$.

(5) Observe that $217 \equiv 2 + 1 + 7 \equiv 1 \bmod 9$. Find a generalization and prove it.

Let $N = a_n 10^n + \ldots + 10a_1 + a_0$ be the representation of an integer in the decimal system. Then $N \equiv a_n + \ldots + a_1 + a_0 \bmod 9$ since $10 \equiv 1 \bmod 9$.