Number Theory - Exercises 2
(for the Working Session of Thursday, March 7)

Lea Terracini

1. . Consider an RSA cryptosystem with $p = 17$, $q = 13$ (hence, $n = pq = 221$), and $e = 35$.

a) What is the value of d?

b) Let (e, n) be the public key of Alice. If we use it to encrypt a message $m = 78$, what is the ciphertext C that Bob send to her?

c) Let d be the private key of Alice. If she receives a ciphertext $C = 65$, what is the original message m?

2. A *decryption exponent* for an RSA public key (n, e) is an integer d with the property that $a^{de} \equiv a \pmod{n}$ for all integers a with $\gcd(a, n) = 1$. Let $n = 99407207$. Assume that an oracle tells you the that

- when $e = 10988423$ the decryption exponent is $d = 26744567$;
- when $e = 25910153$ the decryption exponent is $d = 43278905$;
- when $e = 2635$ the decryption exponent is $d = 52767379$.

Use this information to factor n.

3. Prove that $\varphi(2^n - 1)$ is divisible by n for every $n > 1$.

4. Determine all the primitive roots of 11,19,23.

5.

a) Find all elements in $\mathbb{Z}_{61}^{\times}$ having order 4.

b) Find all elements in $\mathbb{Z}_{35}^{\times}$ having order 4.

6. Let p_n be the n-th prime number. Establish each of the following statements:

a) $p_n \geq 2n - 1$ for $n \geq 5$.

c) The sum

$$\frac{1}{p_1} + \ldots + \frac{1}{p_n}$$

is not an integer number for $n \geq 1$.

7.

a) Let p be a prime ≥ 5. Show that $p \equiv \pm 1 \mod 6$.

b) Use Euclid argument to show that there are infinitely many primes congruent to -1 modulo 6.

8.

a) Show that 5 is a primitive root modulo 17.

b) Find a primitive root modulo $17^2 = 289$.

9. Let $q = 11^3$. How many 84-th roots of unity are there in the finite field $\mathbb{F}_q$?

10. Find the Legendre symbol $\left(\frac{91}{167}\right)$ using the quadratic reciprocity law.