Contact during the exam:
Associate professor Jon Eivind Vatne (90 20 31 17)

Exam in MA1301-Number theory

Wednesday November 30, 2005
Time: 09:00 – 13:00

No aids permitted.
The problem set has two pages.
Give explanations for each answer.

Problem 1

a) Compute $\gcd(788, 116)$. Find all integer solutions to the equation

$$788x + 116y = \gcd(788, 116).$$

b) One day an antiquarian sells some books for 116 kroner each, and buys some books for 788 kroner each. At the end of the day, she is left with 24 kroner more than she had in the morning. What is the minimal number of book she could have sold that day? What is the minimal number of books she could have bought?

Problem 2

a) Find all solutions to the simultaneous congruences

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{6} \\ x &\equiv 6 \pmod{7}. \end{aligned}$$

b) Explain why the set of equations

$$\begin{aligned} 3x + 7y &\equiv 2 \pmod{8} \\ 4x + 5y &\equiv 7 \pmod{8} \end{aligned}$$

has a unique solution modulo 8. Solve the set of equations.

Problem 3

a) You are making an RSA-system in order to receive encrypted messages. You choose $\{n, d\} = \{91, 29\}$ as the secret key. What is the public key $\{n, e\}$?

b) The first secret message you receive is 9. Decipher this message.

Problem 4

a) Formulate Euler's theorem (the proof is not required).

b) Let a be an integer such that $\gcd(a, 5) = 1$. Show that

$$a^{61} \equiv a \pmod{8525}.$$

Hint: $8525 = 5^2.11.31$.

c) Let $n \geq 2$ and a be integers. When is the order of a modulo n defined? What is the definition? What is the order of 8 modulo 19?

Problem 5 Wilson's theorem says that $(p-1)! \equiv -1 \pmod{p}$ for all primes p. Prove Wilson's theorem.

Problem 6 Let (x, y, z) be a primitive Pythagorean triple (so $x^2+y^2 = z^2$ and $\gcd(x, y, z) = 1$). Show that exactly one of the integers x, y, z can be divided by 5. Find an example where $5|x$, and one where $5|z$.

Trygve Johnsen Jon Eivind Vatne