Mathematics, KTH
B.Ek

SF2736 Discrete mathematics
autumn 2015

Problem session 1, 9 November 2015

1. Find the inverse of the element 76 in the ring $\mathbb{Z}_{221}$.

2a. Solve $13x + 18 = 13$ in the ring $\mathbb{Z}_{64}$.

b. Solve $\begin{cases} 7x + 2y = 5 \\ 10x + 7y = 3 \end{cases}$ in the ring $\mathbb{Z}_{13}$.

3. Find all elements b of $\mathbb{Z}_{17}$ such that for at least one $x \in \mathbb{Z}_{17}$:

$$x^2 + 3x + b = 0.$$

4. Find $545^{112} \pmod{23}$ and $545^{112} \pmod{24}$.

5. Show that if p is a prime, then

$$(p-1)! \equiv -1 \pmod{p}.$$

6. Show that for any $k \in \mathbb{Z}$, $3k + 2$ and $5k + 3$ are relatively prime.

7. Find all integers n and m such that $314n + 218m = 12$ with $0 \leq n \leq 200$.

8. Show that for any a, $b \in \mathbb{Z}$ the integers $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are coprime.

9. 2^{29} has (in base 10) 9 digits, all different. Which digit is missing?

10. Call a triple of integers (a, b, c) a **Pythagorean triple** if $a^2 + b^2 = c^2$, i.e. if there is a right triangle with side lengths a, b, c. Examples of Pythagorean triples are $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$ and $(3\,312, 16\,766, 17\,090)$.
Show that if (a, b, c) is a Pythagorean triple

a. at least one of a and b is a multiple of 3,
b. at least one of a, b and c is a multiple of 5,
c. at least one of a and b is a multiple of 4.

11. Find the number of solutions of the equation $x^2 = 1$ in the ring $\mathbb{Z}_{990}$.

12. Solve the equation $(x - 5)(x + 3) = 0$ in the ring $\mathbb{Z}_{56}$.

13. Find all $x \in \mathbb{Z}$ such that $x \equiv 5 \pmod{8}$ and $x \equiv 73 \pmod{81}$.

14. For p a prime and $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}_p$, find the number of solutions $(x_1, x_2, \ldots, x_n) \in (\mathbb{Z}_p)^n$ to the equation

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b.$$

15. Given an RSA-cryptosystem with $n = 1333\,(= 31 \cdot 43)$ and $e = 143$, encrypt the messages $x = 718$ and $x = 719$.
Check the results by finding the correct value for d and decrypting.

16. Use a Fermat primality test to show that the number 63 is not prime.

17. The matrix $\mathbf{H} = \begin{bmatrix} 1&1&1&0&0&0 \\ 1&0&1&1&0&1 \\ 0&1&1&0&1&1 \end{bmatrix}$ is the parity-check matrix of an 1-error-correcting code $\mathcal{C}$.

a. Find all elements of $\mathcal{C}$.
b. Correct the word 011111.
c. How many words cannot be corrected?

18. Three persons are to be fitted with hats. The colours of the hats will be chosen independently, each with equal probability $\frac{1}{2}$ of being red and blue.
With hats on, they will be able to see the colours of the other two hats, but not of their own.
Afterwards each of them will be taken aside and given the chance to guess the colour of his own hat. They will be given a reward if at least one of them guesses correctly and no one wrongly (they may choose not to guess).
They can not hear if or what the others guess, but are allowed to agree on a strategy for their guessing before they are fitted with the hats.
Is there a strategy which would raise their chances to get the reward above the $\frac{1}{2}$ they have if they decide that one of them should guess randomly?