Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, KONSTANTIN ZIEGLER

3. Assignment: Carmichael numbers and the Chinese Remainder Theorem

(Due: Wednesday, 19 November 2008, 13^{40}, b-it bitmax)

Exercise 3.1 (Carmichael numbers). (10 points)

We want to prove, that $N = 561 = 3 \cdot 11 \cdot 17$ is a indeed a Carmichael number, i.e.

$$a^{560} \equiv 1 \pmod{561}$$

for all $a \in \mathbb{Z}_{561}^{\times}$.

(i) Conclude from Fermat's Little Theorem, that for all a coprime to 561 the following holds: $\boxed{4}$

$$a^{560} \equiv 1 \pmod{3}$$
$$a^{560} \equiv 1 \pmod{11}$$
$$a^{560} \equiv 1 \pmod{17}$$

(ii) Use the Chinese Remainder Theorem (as often as necessary) to conclude $\boxed{3}$

$$a^{560} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$$

for all $a \in \mathbb{Z}_{561}^{\times}$.

Recall that the *order* of an element x in a multiplicative group G is the smallest positive integer n, such that

$$x^n = 1.$$

(iii) Consider two relatively prime positive integers $a, b \in \mathbb{Z}_{\geq 2}$. Assume an integer x has order u in the multiplicative group $\mathbb{Z}_a^{\times}$ and order v in the multiplicative group $\mathbb{Z}_b^{\times}$. What is the order of x in the multiplicative group $\mathbb{Z}_{ab}^{\times}$? $\boxed{3}$

Exercise 3.2 (Chinese Remainder Theorem). (10 points)

(i) Consider $21 = 3 \cdot 7$ and fill out a table to visualize the relation between the elements of $\mathbb{Z}_{21}$ and $\mathbb{Z}_7 \times \mathbb{Z}_3$. $\boxed{2}$

(ii) Pick two elements $x, y \in \mathbb{Z}_{21}$ (to make it interesting: the sum of the representing integers shall be larger than 21). First, add them in $\mathbb{Z}_{21}$ and then map to $\mathbb{Z}_7 \times \mathbb{Z}_3$. Second, map both to $\mathbb{Z}_7 \times \mathbb{Z}_3$ and add afterwards. What do you observe? $\boxed{1}$

$\boxed{1}$ (iii) Pick two elements $x, y \in \mathbb{Z}_{21}$ (to make it interesting: the product of the representing integers shall be larger than 21). First, multiply them in $\mathbb{Z}_{21}$ and then map to $\mathbb{Z}_7 \times \mathbb{Z}_3$. Second, map both to $\mathbb{Z}_7 \times \mathbb{Z}_3$ and multiply afterwards. What do you observe?

Note: a map having the properties observed in (ii) and (iii) is called a *ring homomorphism*.

$\boxed{2}$ (iv) Mark all the invertible elements in $\mathbb{Z}_7$, $\mathbb{Z}_3$, and $\mathbb{Z}_{21}$. What is their relationship?

Now consider two relatively prime positive integers $a, b \in \mathbb{Z}_{\geq 2}$.

$\boxed{1}$ (v) Let x be any integer and suppose $x \pmod{ab}$ is invertible. Prove that $x \pmod{a}$ and $x \pmod{b}$ are also invertible.

$\boxed{2}$ (vi) Assume that an integer y is invertible modulo a and modulo b. Prove that y is then invertible modulo ab.

$\boxed{1}$ (vii) Conclude that there is a bijection between $\mathbb{Z}_{ab}^{\times}$ and $\mathbb{Z}_a^{\times} \times \mathbb{Z}_b^{\times}$.