UE Discrete Mathematics

Exercises for January 8/9, 2014

91) Use the Chinese remainder theorem to solve the following system of congruence relations:

$$\begin{aligned} 5x &\equiv 8\ (32) \\ 14x &\equiv 2\ (22) \\ 9x &\equiv 3\ (15) \end{aligned}$$

92) Let $(n, e) = (3233, 49)$ be a public RSA key. Compute the decryption key d.

93) Use the key of exercise 92) to encrypt the string „`COMPUTER`“. Decompose the string into blocks of length 2 and apply the mapping $\mathtt{A} \mapsto 01,\ \mathtt{B} \mapsto 02, \ldots,\ \mathtt{Z} \mapsto 26$.

94) Prove that the identity

$$\varphi(m \cdot n) = \varphi(m)\varphi(n)\frac{\gcd(m,n)}{\varphi(\gcd(m,n))}$$

holds for all $m, n \in \mathbb{N}^+$. φ denotes Euler's totient function.

95) Let λ and φ denote the Carmichael function and Euler's totient function, respectively. Compute $\lambda(172872)$ and $\varphi(172872)$.

96) Let (e, n) and (d, n) be Bob's public and private RSA key, respectively. Suppose that Bob sends an encrypted message c and Alice wants to find out the original message m. She has the idea to send Bob a message and ask him to sign it. How can she find out m?

Hint: Pick a random integer r and consider the message $r^e c \mod n$.

97) Let $A_{d,n} = \{x \mid 1 \le x \le n \text{ and } \gcd(x, n) = d\}$

(a) Show that $\bigcup_{d|n} A_{d,n} = \{1, 2, \ldots, n\}$.

(b) Show that $|A_{d,n}| = |A_{1,n/d}|$. Hint: First show that $\gcd(k, n) = d$ if and only if $\gcd\left(\frac{k}{d}, \frac{n}{d}\right) = 1$ and use this to construct a bijection.

(c) Use (b) to show that

$$\sum_{d|n} \varphi(d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$$

where φ denotes Euler's totient function.

98) Prove: If G is a finite group and $a \in G$ an element with $\mathrm{ord}_G(a) = r$. Then $\mathrm{ord}_G(a^k) = r/\gcd(r, k)$.

99) Let G be a finite group and $a \in G$ an element for which $\mathrm{ord}_G(a)$ is maximal. Prove that for all $b \in G$ the order $\mathrm{ord}_G(b)$ is a divisor of $\mathrm{ord}_G(a)$.

100) Show that $m \mid n$ implies $\lambda(m) \mid \lambda(n)$ where λ denotes the Carmichael function.

Hint: Prove first that $a_i \mid b_i$ for $i = 1, \ldots, k$ implies $\mathrm{lcm}(a_1, a_2, \ldots, a_k) \mid \mathrm{lcm}(b_1, b_2, \ldots, b_k)$.