Vietnamese-German University
Computer Science study program
Course: Algebra

Exercise Sheet: Number Theory

1. Find the last digit of the following sum using the remainders of 10.

   (a)
   $$2403 + 791 + 688 + 4339$$

   (b) $1 + 11^{10} + 111^{10} + \cdots + \underbrace{11\overset{10}{\cdots}1}_{100 times}$

2. Find

   (a) $14 \mod 9$
   (b) $-1 \mod 9$
   (c) $-11 \mod 9$
   (d) $21.38 \mod 9$
   (e) $21 + 38 \mod 9$
   (f) $2^5 \mod 9$
   (g) $2^{2016} \mod 9$

3. Find

   (a) $7^{121} \mod 13$
   (b) $2^{340} \mod 11$
   (c) $5^{2003} \mod 7$
   (d) $5^{2003} \mod 11$
   (e) $5^{2003} \mod 13$
   (f) $5^{2003} \mod 7 \cdot 11 \cdot 13$

4. Jesper has 44 boxes of soda in his truck. The cans of soda in each box are packed oddly so that there are 113 cans of soda in each box. Jesper plans to pack the sodas into cases of 12 cans to sell. After making as many complete cases as possible, how many sodas will Jesper have leftover?
   Use modular arithmetic to solve the problem.

5. Which are prime, which are composite?

   (a) 119
   (b) $n! - 1$
   (c) $2^{2000} + 1$
   (d) $n^4 + 4$

6. Show that if $2^n - 1$ is prime, then n is prime.

7. Determine whether the integers in each of these sets are pairwise relatively prime

   (a) $7, 8, 9, 11$

   (b) $14, 15, 21$

   (c) $2^{35} - 1$ and $2^{2015} - 1$

8. The value of the Euler function ϕ at a positive integer n is defined to be the number of positive integers less than or equal to n that are relatively prime to n. Find the following

   a) $\phi(4), \phi(10), \phi(13)$

   b) $\phi(p^k)$ where p is a prime number and k is a positive integer

   c) $\phi(pq)$ where p and q are prime numbers.

   d*) $\phi(p_1^{a_1} p_2^{a_2} \dots p_n^{a_n})$ where p_i are distinct prime numbers.

9. What are the greatest common divisors and the least common multiple of these pairs of integers?

   (a) $3^7 \cdot 5^3 \cdot 7^3$ and $3^9 \cdot 5^2 \cdot 11^2$

   (b) 1000 and 625

   (c) $3^{13} \cdot 5^{17}$ and $2^{12} \cdot 7^{21}$

   (d) 1111 and 0.

10. Find the greatest common divisors of the following pairs using Euclid's algorithm and prime factorization theorem.

    (a) $\gcd(12, 18)$

    (b) $\gcd(108, 30)$

    (c) $\gcd(111, 201)$

    (d) $\gcd(210, 126)$

    (e) $\gcd(1000, 5040)$

    (f) $\gcd(54321, 9876)$

    (g) $\gcd(67890, 12345)$

    (h) $\gcd(12345, 54321)$

11. Express the greatest common divisor as a linear combination of original numbers

    (a) $5, 11$

    (b) $21, 44$

    (c) $36, 48$

    (d) $34, 55$

    (e) $117, 213$

12. Encrypt the message HERE IS A MESSAGE using a Caesar cipher in which each letter is shifted three places to the right.

13. Propose or writing a computer program to find the multiplicative inverse of a number a in $\mathbb{Z}_n$.

14. If $a \cdot 133 - m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

15. Determine whether every nonzero element of $\mathbb{Z}_n$ has a multiplicative inverse for $n = 10$ and $n = 11$. How many elements $a \in \mathbb{Z}_{10}$ such that $a \cdot_{10} 2 = 1$?

16. Using the inverse-solving in Euclid's division to find multiplicative inverse of

    (a) $5 \in \mathbb{Z}_{11}$
    (b) $3 \in \mathbb{Z}_{10}$
    (c) $2 \in \mathbb{Z}_{10}$
    (d) $16 \in \mathbb{Z}_{103}$
    (e) $22 \in \mathbb{Z}_{31}$

17. Solve the equations

    (a) $5 \cdot_{11} x = 1$ in $\mathbb{Z}_{11}$
    (b) $5 \cdot_{11} x = 8$ in $\mathbb{Z}_{11}$

18. What is the value of the division 1 by 4 in $\mathbb{Z}_9$?

19. By multiplying a number x times $487 \in \mathbb{Z}_{30031}$ we obtain 13008. If you know how to find such number x, do so. If not, explain why the problem seems difficult to do by hand.

20. Knowing that Alice sent a message to Bob using multiplication mod $n = 103$ with the common key $a = 16$. Assume that Bob receives the message $m = 21$. What is the original message that Alice sent Bob?

21. In Turing's cipher, version 1, suppose that the adversary got two numeric encrypted message $y_1 = 4307$ and $y_2 = 7373$.

    (a) Find the common private key e.
    (b) Decrypt the message 10877.

22. In Turing's cipher, version 2, given modulus $n = 30$.

    (a) Find the non-trivial smallest valid private key;
    (b) Encrypt the numeric message $x = 17$;
    (c) Decrypt the message $y = 19$.

23. In Turing's cipher, version 2 given modulus $n = 63$. Suppose that the adversary knows both plaintext and ciphertext $x = 55$ and $y = 25$ respectively.

(a) Find the common private key e;

(b) Decrypt the numeric message $y = 31$.

24. Is $0 - 84 - 930149 - X$ a valid ISBN-10?

25. The first nine digits of the ISBN-10 for the fifth edition of the book "DMAäre $0 - 07 - 119881$. What is its check digit?

26. Encrypt the message CRIZZLY BEARS using blocks of five letters and the transposition cipher based on the permutation of $\{1, 2, 3, 4, 5\}$ with $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 1$, $\sigma(4) = 2$, $\sigma(5) = 4$

27. Decrypt the message EABW EFRO ATMR ASIN which is the cipher text produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation σ of $\{1, 2, 3, 4\}$ defined by $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$.

28. (small RSA crypto-system). Given the modulus $n = 33$.

(a) What are prime factors p and q of n.

(b) Find Euler's totient function $\phi(n)$ of n.

(c) Find the two non-trivial smallest valid public exponents e_1 and e_2 for the RSA with public modulus n;

(d) Encrypt numeric message $x = 4$ given public exponent e_1 above;

(e) Decrypt numeric message $y = 31$ given public exponent e_2 above.

29. Suppose the RSA modulus $n = p.q$ is the product of distinct 200 digit primes p and q. A message $m \in \mathbb{Z}_n$ is called *dangerous* if $\gcd(m, n) = p$, because such an n can be used to factor n and so crack RSA. Circle the best estimate of the fraction of messages in $\mathbb{Z}_n$ that are dangerous:

$$\frac{1}{200}, \quad \frac{1}{400}, \quad \frac{1}{200^{10}}, \quad \frac{1}{10^{200}}, \quad \frac{1}{400^{10}}, \quad \frac{1}{10^{400}}.$$

30. Implement the fast exponentiation for x^{60}.

31. Bob and Alice want to choose a key that they can use for cryptography, but all they have to communicate is a bugged phone line. Bob proposes thay they choose a secrete number, a for Alice and b for Bob. They also choose, over the phone a prime number p with more digits than any key they want to use, and one more number q. Bob will send Alice $bq \mod p$, and Alice will send Bob $aq \mod p$. Their key (which they keep secrete) will then be $abq \mod p$. Here we don't worry about the details of how they use their key, only with how they choose it. As Bob explains, their wire tapper will know $p, q, aq \mod p$, and $bq \mod p$, but will not know a or b, so their key should be safe. In this scheme

safe, that is can the wiretapper compute $abq \mod p$? If so, how does she do it? Alice says "You know, the scheme sounds good, but would not it be more complicated for the wire tapper if I send you $q^a \mod p$, you send me $q^b \mod p$ and we use $q^{ab} \mod p$ as our key." In this case, can you think of a way for the wire tapper to compute $q^{ab} \mod p$? If so, how can you do it? If not, what is the stumbling block?