Number Theory/Cryptography (part 1 of CSC 282)

http://www.cs.rochester.edu/~stefanko/Teaching/11CS282

1 Schedule

The homework is **due Sep 8**
Graded homework will be available at noon **Sep 9, noon**.
EXAM #1 will be on **Tuesday, Sep. 13**.

2 List of algorithms covered in the class

(B-basic, I-intermediate, A-advanced):

B: Addition (p.11, DSV).
B: Multiplication (p.15, DSV).
B: Division (p.15, DSV).
B: Modular exponentiation (p.19, DSV).
B: Euclid's algorithm (p.20, DSV).
I: Extended Euclid's algorithm (p.21, DSV).
A: Primality testing (p.25, DSV).
A: Generating random primes (p.28, DSV).
A: RSA (p.33, DSV).

3 Basic material

Important concepts, problems, theorems, and algorithms:

- Modular arithmetic, Fermat's little theorem.

  Theorem: Let p be a prime and let a be an integer such that $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

  Theorem: Let p be a prime and let a be an integer. Then $a^p \equiv a \pmod{p}$.

Simple (computational) questions:

- Compute $a^b \bmod c$. (c will be a prime smaller than 20.)
- Trace the execution of Euclid's gcd algorithm.
- Compute the multiplicative inverse of a modulo b.
- Apply Fermat's little theorem in a computation (see problems 1.1, 1.4, 1.5, below).

Example problems (<u>solve, but do NOT turn in</u>):

1.1 Compute $3^{80} \mod 5$.

1.2 Compute $\gcd(30, 81)$. Compute $\gcd(55, 34)$. Use Euclid's gcd algorithm. Show all steps.

1.3 Compute the multiplicative inverse of 26 modulo 677.

1.4 Is $4^{200} - 9^{100}$ divisible by 35? Use Fermat's little theorem to prove your answer.

1.5 What is $3^{3^{100}} \bmod 5$? (as usual, a^{b^c} is a raised to the b^c-th power).

1.6 Prove that for every integer x, either $x^2 \equiv 0 \pmod 4$ or $x^2 \equiv 1 \pmod 4$.

1.7 Let p, q be two different primes. Let x, y be such that $x \equiv y \pmod p$ and $x \equiv y \pmod q$. Prove that $x \equiv y \pmod{pq}$.

4 Basic Homework - solve and turn in

1.8 (**due Sep 8**) Solve the following system of congruences:

$$x \equiv 20 \pmod{21},$$
$$x \equiv 21 \pmod{22},$$
$$x \equiv 22 \pmod{23}.$$

That is, find $x \in \{0, \ldots, 10625\}$ that satisfies all 3 congruences above. (HINT: Chinese remainder theorem.)

1.9 (**due Sep 8**) Let p be a prime and let a, b be two integers such that $a^2 \equiv b^2 \pmod p$. Prove that either $a \equiv b \pmod p$ or $a \equiv -b \pmod p$. (HINT: you will need to use the following fact about primes and divisibility. If p is a prime and $p \mid cd$ then $p \mid c$ or $p \mid d$.)

1.10 (**due Sep 8**) For each of the following—prove or disprove (clearly state which of the two are you doing):

- For all $x \in \mathbb{Z}$ such that $\gcd(x, 19) = 1$ we have $x^{18} \equiv 1 \pmod{19}$.
- For all $x \in \mathbb{Z}$ such that $\gcd(x, 21) = 1$ we have $x^{18} \equiv 1 \pmod{21}$.
- For all $x \in \mathbb{Z}$ we have $x^{37} \equiv x \pmod{37}$.
- For all $x \in \mathbb{Z}$ we have $x^{37} \equiv x \pmod{35}$.

5 Advanced Homework solve and turn in

Please, make sure that the basic homework and the advanced homework are on separate sheets of paper.

1.11 (**due Sep 8**) Let p be a prime such that $p \equiv 3 \pmod 4$. We would like to have an algorithm which on input x computes the square root of x, that is, y such that $y^2 \equiv x \pmod p$. Show that we can let $y := x^{(p+1)/4} \pmod p$.

1.12 (**due Sep 8**) Let x, y be unknown positive integers. Let $A = xy$ and $B = x + y$. Give a polynomial-time algorithm which on input A, B computes x, y. Clearly state and analyze the running time of your algorithm.

1.13 (**due Sep 8**) Professor A designed a black-box which on input a computes a^2 in time $O(\log a)$. We would like to use the black-box to multiply numbers, i. e., on input a, b we want to compute ab. We want our algorithm to run in time $O(\log(ab))$.

a) Give such an algorithm.

b) Suppose now, that instead of $x \mapsto x^2$ black-box, we have $x \mapsto x^3$ black-box. Show how we can use the new black-box to multiply numbers a, b in time $O(\log(ab))$.

c) Suppose now, that instead of $x \mapsto x^2$ black-box, we have $x \mapsto x^4$ black-box. Show how we can use the new black-box to multiply numbers a, b in time $O(\log(ab))$.

In parts a), b), c) you can assume that we can add two numbers c, d in $O(\log(cd))$-time. You can also assume that for any constant f we can divide d by f in $O(\log d)$-time.

1.14 (**due Sep 8**) Fibonnaci numbers are defined as follows: $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Give a polynomial-time algorithm which on input n and M outputs ($F_n \mod M$). (Note that the input length is $\Theta(\log n + \log M)$, and your algorithm has to run in time polynomial in the input length).

6 Additional problems from the book (do NOT turn in)

Try to solve the following problems. A few of them will be on the quiz.

- 1.1, 1.4, 1.5, 1.10, 1.11, 1.14, 1.15, 1.19, 1.20, 1.22, 1.23, 1.25, 1.26, 1.31, 1.32, 1.37, 1.39.

7 Additional problems (do NOT turn in)

Solve the problems below; use the answer key below to check your answers.

Definitions: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ denotes the set of **integers**, $\mathbb{N} = \{1, 2, 3, \dots\}$ denotes the set of **natural numbers** (which we define to be positive integers). For $a, b \in \mathbb{Z}$ we say a **divides** b (notation: $a \mid b$) if there exists $c \in \mathbb{Z}$ such that $b = ac$. For $a, b, m \in Z$ we say a is **congruent** to b modulo m (notation: $a \equiv b \pmod{m}$) if $m \mid (a - b)$. We say that a natural number n is a **prime** if there are exactly 2 natural numbers that divide n (they are 1 and n, with $n \neq 1$). For a natural number m we let $\mathbb{Z}_m^* = \{a \in \{1, \dots, m-1\} \mid \gcd(a, m) = 1\}$, that is, Z_m^* are the numbers from $\{1, \dots, m-1\}$ that are *co-prime* with m.

---

1. If p, q are different primes then $\gcd(p, q) = 1$. TRUE - FALSE

2. If $2 \mid (a + b)$ then $a \equiv b \pmod{2}$. TRUE - FALSE

3. If p is a prime and $p \mid (a + b)$ then $a \equiv b \pmod{p}$. TRUE - FALSE

4. If $m \mid (a - b)$ then $a \equiv b \pmod{m}$. TRUE - FALSE

5. If $ab \equiv 1 \mod c$ then $\gcd(a, c) = 1$. TRUE - FALSE

6. If $ab \equiv 1 \mod c$ then $\gcd(a, b) = 1$. TRUE - FALSE

7. If $a \mid b$ and $b \mid c$ then $a \mid c$. TRUE - FALSE

8. If $a \mid bc$ then $a \mid b$ or $a \mid c$. TRUE - FALSE

9. If p is a prime, $p \mid (b + c)$, and $p \mid (b - c)$ then $p \mid c$. TRUE - FALSE

10. If $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$ then $\gcd(ab, c) = 1$. TRUE - FALSE

11. If $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$ then $\gcd(a + b, c) = 1$. TRUE - FALSE

12. If $\gcd(a, b) = 1$ and $\gcd(c, d) = 1$ then $\gcd(ac, bd) = 1$. TRUE - FALSE

13. If p is a prime and $p \mid a^2$ then $p \mid a$. TRUE - FALSE

14. If p is an odd prime then $3^{(p-1)/2} \equiv 1 \pmod{p}$. TRUE - FALSE

15. If p is an odd prime then $4^{(p-1)/2} \equiv 1 \pmod{p}$. TRUE - FALSE

16. If p is an odd prime, $p \mid (b + c)$, and $p \mid (b^2 + c^2)$ then $p \mid c$. TRUE - FALSE

17. If $a \mid c$ and $b \mid c$ then $ab \mid c$. TRUE - FALSE

18. Let p be a prime. If $a^k \equiv 1 \pmod{p}$ and $b^k \equiv 1 \pmod{p}$ then $(ab)^k \equiv 1 \pmod{p}$.
TRUE - FALSE

19. Let $m \geq 2$. If $a^k \equiv 1 \pmod{m}$ and $b^k \equiv 1 \pmod{m}$ then $(ab)^k \equiv 1 \pmod{m}$.
TRUE - FALSE

20. Let $m \geq 2$. If for all $a \in \{1, \ldots, m-1\}$ we have $a^{m-1} \equiv 1 \pmod{m}$ then m is a prime.
TRUE - FALSE

21. Let $m \geq 2$. If for all $a \in \mathbb{Z}_m^*$ we have $a^{m-1} \equiv 1 \pmod{m}$ then m is a prime.
TRUE - FALSE

22. Let p be a prime. If $a \equiv 1 \pmod{p-1}$ and $\gcd(p, b) = 1$ then $b^a \equiv b \pmod{p}$.
TRUE - FALSE

23. Let p be a prime. If $a \equiv 1 \pmod{p-1}$ and $\gcd(p, b) = 1$ then $a^b \equiv a \pmod{p}$.
TRUE - FALSE

24. Let p be a prime. If $a \equiv 1 \pmod{p}$ and $\gcd(p-1, b) = 1$ then $b^a \equiv b \pmod{p}$.
TRUE - FALSE

25. Let p be a prime. If $a \equiv 1 \pmod{p}$ and $\gcd(p-1, b) = 1$ then $a^b \equiv a \pmod{p}$.
TRUE - FALSE

26. If $2 \mid (a+b)$ then $a^2 \equiv b^2 \pmod{2}$. TRUE - FALSE

27. Assume $a, b, c \in \mathbb{N}$. If $a^b \equiv 1 \pmod{c}$ then $\gcd(a, c) = 1$. TRUE - FALSE

28. Assume $a, b, c \in \mathbb{N}$. If $a^b \equiv 1 \pmod{c}$ then $\gcd(b, c) = 1$. TRUE - FALSE

29. If p is an odd prime then $4^{(p+1)/2} \equiv 4 \pmod{p}$. TRUE - FALSE

30. If $\gcd(a+b, c) = 1$ and $\gcd(b, c) = 1$ then $\gcd(a, c) = 1$. TRUE - FALSE

31. Let p be a prime, $a \in \{2, \ldots, p-1\}$, and $b \in \mathbb{N}$. If $a^b \equiv a \pmod{p}$ then $\gcd(b, p-1) = 1$.
TRUE - FALSE

Solutions.

1. If p, q are different primes then $\gcd(p,q) = 1$. **TRUE** - FALSE

   (WHY: w.l.o.g. $p < q$; assume, for the sake of contradiction, that $\gcd(p,q) = a > 1$; then $a \mid q$, yet $a \neq 1$ and $a \neq q$ (since $a \leq p < q$), contradicting the assumption that q is a prime.)

2. If $2 \mid (a+b)$ then $a \equiv b \pmod 2$. **TRUE** - FALSE

   (WHY: if $2 \mid (a+b)$ then either both a, b are even or both a, b are odd; in both cases $a \equiv b \pmod 2$.)

3. If p is a prime and $p \mid (a+b)$ then $a \equiv b \pmod p$. TRUE - **FALSE**

   (WHY: $p = 3$, $a = 1$, $b = 2$ is a counterexample.)

4. If $m \mid (a-b)$ then $a \equiv b \pmod m$. **TRUE** - FALSE

   (WHY: definition of $a \equiv b \pmod m$.)

5. If $ab \equiv 1 \mod c$ then $\gcd(a,c) = 1$. **TRUE** - FALSE

   (WHY: assume, for the sake of contradiction, that $\gcd(a,c) = t > 1$; then $t \mid a$ and $t \mid (1-ab)$, hence $t \mid 1$, and hence $t = 1$, a contradiction (we used the fact that $t \mid A$ and $t \mid B$ implies $t \mid (A+B)$ (used with $A = ab$ and $B = 1 - ab$).)

6. If $ab \equiv 1 \mod c$ then $\gcd(a,b) = 1$. TRUE - **FALSE**

   (WHY: $p = 7$, $a = 2$, $b = 4$ is a counterexample.)

7. If $a \mid b$ and $b \mid c$ then $a \mid c$. **TRUE** - FALSE

   (WHY: we have $X \in \mathbb{Z}$ such that $b = aX$ and $Y \in \mathbb{Z}$ such that $c = bY$; hence $c = a(XY)$, thus, $a \mid c$.)

8. If $a \mid bc$ then $a \mid b$ or $a \mid c$. TRUE - **FALSE**

   (WHY: $a = 4, b = 2, c = 2$ is a counterexample.)

9. If p is a prime, $p \mid (b+c)$, and $p \mid (b-c)$ then $p \mid c$. TRUE - **FALSE**

   (WHY: $p = 2, a = 1, b = 1$ is a counterexample.)

10. If $\gcd(a,c) = 1$ and $\gcd(b,c) = 1$ then $\gcd(ab,c) = 1$. **TRUE** - FALSE

    (WHY: no prime divides both a and c; no prime divides both b and c; hence no prime divides both ab and c (since the set of primes dividing ab is the union of the set of primes dividing a and the set of primes dividing b).)

11. If $\gcd(a,c)=1$ and $\gcd(b,c)=1$ then $\gcd(a+b,c)=1$. TRUE - [FALSE]

(WHY: $a=1, b=1, c=2$ is a counterexample.)

12. If $\gcd(a,b)=1$ and $\gcd(c,d)=1$ then $\gcd(ac,bd)=1$. TRUE - [FALSE]

(WHY: $a=1, b=2, c=2, d=1$ is a counterexample.)

13. If p is a prime and $p \mid a^2$ then $p \mid a$. [TRUE] - FALSE

(WHY: this follows from that fact that if p is a prime and $p \mid XY$ then $p \mid X$ or $p \mid Y$ (used with $X=Y=a$).)

14. If p is an odd prime then $3^{(p-1)/2} \equiv 1 \pmod{p}$. TRUE - [FALSE]

(WHY: $p=3$ is a counterexample.)

15. If p is an odd prime then $4^{(p-1)/2} \equiv 1 \pmod{p}$. [TRUE] - FALSE

(WHY: since $4=2^2$ we have $4^{(p-1)/2} \equiv 2^{p-1} \equiv 1 \pmod{p}$, the last congruence follows from Fermat's little theorem.)

16. If p is an odd prime, $p \mid (b+c)$, and $p \mid (b^2+c^2)$ then $p \mid c$. [TRUE] - FALSE

(WHY: $p \mid (b+c)$ implies $p \mid (b^2-c^2)$, which combined with $p \mid (b^2+c^2)$ implies $p \mid 2c^2$; now since p is odd we cannot have $p \mid 2$ and hence $p \mid c^2$ which, in turn, implies $p \mid c$.)

17. If $a \mid c$ and $b \mid c$ then $ab \mid c$. TRUE - [FALSE]

(WHY: $a=2, b=2, c=2$ is a counterexample.)

18. Let p be a prime. If $a^k \equiv 1 \pmod{p}$ and $b^k \equiv 1 \pmod{p}$ then $(ab)^k \equiv 1 \pmod{p}$.
[TRUE] - FALSE

(WHY: see the next problem.)

19. Let $m \geq 2$. If $a^k \equiv 1 \pmod{m}$ and $b^k \equiv 1 \pmod{m}$ then $(ab)^k \equiv 1 \pmod{m}$.
[TRUE] - FALSE

(WHY: $(ab)^k = a^k b^k$; $A \equiv B \pmod{m}$ and $C \equiv D \pmod{m}$ implies $AC \equiv BD \pmod{m}$.)

20. Let $m \geq 2$. If for all $a \in \{1, \ldots, m-1\}$ we have $a^{m-1} \equiv 1 \pmod{m}$ then m is a prime.
[TRUE] - FALSE

(WHY: if m is not a prime then take $a \mid m$ where $a \in \{2, \ldots, m-1\}$; then $a \mid a^{m-1}$; then $a \nmid (a^{m-1}-1)$; hence $m \nmid (a^{m-1}-1)$ and hence $a^{m-1} \not\equiv 1 \pmod{m}$.)

21. Let $m \geq 2$. If for all $a \in \mathbb{Z}_m^*$ we have $a^{m-1} \equiv 1 \pmod{m}$ then m is a prime.
TRUE - [FALSE]

(WHY: Carmichael numbers, for example $m=561$, are a counterexample.)

22. Let p be a prime. If $a \equiv 1 \pmod{p-1}$ and $\gcd(p,b) = 1$ then $b^a \equiv b \pmod{p}$.
TRUE - FALSE

(WHY: We have $a = 1 + k(p-1)$ for some $k \in \mathbb{Z}$; then $b^a \equiv b(b^{p-1})^k \equiv b \pmod{p}$, using Fermat's little theorem in the last congruence.)

23. Let p be a prime. If $a \equiv 1 \pmod{p-1}$ and $\gcd(p,b) = 1$ then $a^b \equiv a \pmod{p}$.
TRUE - FALSE

(WHY: $p = 3, a = 5, b = 2$ is a counterexample.)

24. Let p be a prime. If $a \equiv 1 \pmod{p}$ and $\gcd(p-1,b) = 1$ then $b^a \equiv b \pmod{p}$.
TRUE - FALSE

(WHY: $p = 3, a = 4, b = 5$ is a counterexample.)

25. Let p be a prime. If $a \equiv 1 \pmod{p}$ and $\gcd(p-1,b) = 1$ then $a^b \equiv a \pmod{p}$.
TRUE - FALSE

(WHY: If $a \equiv 1 \pmod{p}$ then $a^b \equiv 1 \pmod{p}$ for any $b \in \mathbb{N}$.)

26. If $2 \mid (a+b)$ then $a^2 \equiv b^2 \pmod{2}$.
TRUE - FALSE

(WHY: if $2|(a+b)$ then either both a, b are even or both a, b are odd; in both cases $a^2 \equiv b^2 \pmod{2}$.)

27. Assume $a, b, c \in \mathbb{N}$. If $a^b \equiv 1 \pmod{c}$ then $\gcd(a,c) = 1$.
TRUE - FALSE

(WHY: if $\gcd(a,c) = t > 1$ then $t \mid a^b$; hence $t \nmid (a^b - 1)$; hence $c \nmid (a^b - 1)$; hence $a^b \not\equiv 1 \pmod{c}$.)

28. Assume $a, b, c \in \mathbb{N}$. If $a^b \equiv 1 \pmod{c}$ then $\gcd(b,c) = 1$.
TRUE - FALSE

(WHY: $a = 1, b = 2, c = 2$ is a counterexample.)

29. If p is an odd prime then $4^{(p+1)/2} \equiv 4 \pmod{p}$.
TRUE - FALSE

(WHY: since $4 = 2^2$ we have $4^{(p+1)/2} \equiv 2^{p+1} \equiv 2^2 \pmod{p}$, where in the last congruence we used Fermat's little theorem)

30. If $\gcd(a+b,c) = 1$ and $\gcd(b,c) = 1$ then $\gcd(a,c) = 1$.
TRUE - FALSE

(WHY: $a = 2, b = 1, c = 2$ is a counterexample)

31. Let p be a prime, $a \in \{2, \ldots, p-1\}$, and $b \in \mathbb{N}$. If $a^b \equiv a \pmod{p}$ then $\gcd(b, p-1) = 1$.
TRUE - FALSE

(WHY: $p = 7, a = 2, b = 4$ is a counterexample)