1  Schedule

The homework is **due Sep 11, 2008**.
The QUIZ will be on **Tuesday, Sep. 16**.

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 \( a^{p-1} \equiv 1 \pmod{p} \).

- Fermat’s little theorem.
  
  **Theorem:** Let \( p \) be a prime and let \( a \) be an integer. Then \( a^p \equiv a \pmod{p} \).

**Testing method:**

- Compute \( a^b \mod c \). (\( c \) 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 (homework):**

1.1 *(due Sep 11, 2008)* Compute \( 2^{101} \mod 5 \).

1.2 *(due Sep 11, 2008)* Compute \( \gcd(30, 105) \). Compute \( \gcd(89, 55) \). Use Euclid’s gcd algorithm. Show all steps.

1.3 *(due Sep 11, 2008)* Compute the multiplicative inverse of 31 modulo 872.

1.4 *(due Sep 11, 2008)* Is \( 4^{312} - 9^{1200} \) divisible by 35? Use Fermat’s little theorem to prove your answer.

1.5 *(due Sep 11, 2008)* What is \( 2^{2^{100}} \mod 5 \)? (as usual, \( a^{b^c} \) is \( a \) raised to the \( b^c \)-th power).

1.6 *(due Sep 11, 2008)* Prove that for every integer \( x \), either \( x^2 \equiv 0 \pmod{4} \) or \( x^2 \equiv 1 \pmod{4} \).
1.7 (due Sep 11, 2008) 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 $x \equiv y \pmod{pq}$.

1.8 (due Sep 11, 2008) 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 $x^{37} \equiv x \pmod{35}$.

4 Additional homework

1.9 (due Sep 11, 2008) Solve the following system of congruences:

\[
\begin{align*}
  x & \equiv 7 \pmod{11} \\
  x & \equiv 8 \pmod{12} \\
  x & \equiv 9 \pmod{13}
\end{align*}
\]

(HINT: Chinese remainder theorem.)

1.10 (due Sep 11, 2008) 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 $x, y$.

1.11 (due Sep 11, 2008) 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 $a \equiv -b \pmod{p}$. Clearly state where in your proof you used the assumption that $p$ is a prime.

1.12 (due Sep 11, 2008) [BONUS PROBLEM] 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.

5 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.