Indian Institute of Technology Kharagpur

CS60094: Computational Number Theory, Spring 2018-19
Mid-Semester Examination

26th February, 2019 | CSE 107/108, 2PM – 4PM | Total marks: 60

Answer all questions. If you make any assumptions, state them upfront. Provide concise answers.

---

1. Suppose that $\gcd(r_0, r_1)$ is computed by the repeated Euclidean division algorithm. Assume $r_0 > r_1 > 0$. Let r_{i+1} denote the remainder obtained by the i-th division (that is, in the i-th iteration of the Euclidean loop). So the computation proceeds as $\gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots$ with $r_0 > r_1 > r_2 > \cdots > r_k > r_{k+1} = 0$ for some $k \geq 1$.

   If the computation of $\gcd(r_0, r_1)$ requires exactly k Euclidean divisions, show that $r_0 \geq F_{k+1}$ and $r_1 \geq F_k$. Here, F_n is the n-th Fibonacci number: $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. **[10]**

   Solution: Let $q_2, q_3, \ldots, q_{k+1}$ denote the quotients obtained in the k Euclidean divisions required for the computation of $\gcd(r_0, r_1)$. Clearly $q_i \geq 1$ for each $i \in [2, k+1]$. We have $r_{k+1} = 0$ and $r_k > r_{k+1}$ where r_k is an integer. As a result $r_{k+1} \geq 0 = F_0$, $r_k \geq 1 = F_1$ and $r_{k-1} \geq q_{k+1} r_k + r_{k+1} \geq r_k + r_{k+1} = F_1 + F_0 = F_2$. For some $i \in [1, k+1]$, assume $r_j \geq F_{k+1-j}$ for all $j \geq i$. We can write $r_{i-1} = q_{i+1} r_i + r_{i+1}$ for some $q_{i+1} \geq 1$ and $0 \leq r_{i+1} < r_i$. It follows from the induction hypothesis that $r_{i-1} \geq r_i + r_{i+1} \geq F_{k+1-i} + F_{k+1-(i+1)} = F_{k+1-i} + F_{k-i} = F_{k+2-i} = F_{k+1-(i-1)}$. Since this holds for any $i \in [1, k+1]$, it follows that $r_0 \geq F_{k+1}$ and $r_1 \geq F_k$.

2. Let $m \in \mathbb{N}$ be a large modulus and let $a, b \in \mathbb{Z}_m$. Consider a sequence of integers modulo m, $x_1, x_2, x_3, \ldots$ computed by first choosing x_0 from $\mathbb{Z}_m$ and recursively generating $x_i \leftarrow a x_{i-1} + b \pmod m$ for $i \geq 1$. Describe an algorithm to compute x_n given (x_0, a, b, n) that runs in time polynomial in both $\log_2 m$ and $\log_2 n$. Assume $(a-1) \in \mathbb{Z}_m^*$. **[10]**

   Solution:

$$
\begin{aligned}
x_n &= a x_{n-1} + b \pmod m \\
&= a(a x_{n-2} + b) + b \pmod m \\
&= a^2 (a x_{n-3} + b) + (a+1) b \pmod m \\
&= \cdots \\
&= a^n x_0 + (a^{n-1} + a^{n-2} + \cdots + a + 1) b \pmod m \\
&= a^n x_0 + \left(\frac{a^n - 1}{a - 1} \right) b \pmod m
\end{aligned}
$$

   As $a - 1$ is invertible in $\mathbb{Z}_m^*$, we can compute x_n as $a^n x_0 + (a^n - 1)(a-1)^{-1} b \pmod m$ The modular exponentiation procedure to compute a takes $O(\log n \log^2 m)$ time. Computing requires $O(\log^2 m)$ time. Computing x_n requires computation of $a^n \pmod m$, $(a-1)^{-1} \pmod m$ and two multiplications modolo m taking $O(\log^2 m)$ each. Total time required is $O(\log n \log^2 m)$ which is polynomial in $\log m$ and $\log n$.

3. Let $\sigma(n)$ denote the sum of all positive integral divisors of $n \in \mathbb{N}$. For example, $\sigma(20) = 1+2+4+5+10+20 = 42$. Let $n = pq$ with two distinct primes p, q. Devise a polynomial time algorithm to compute p, q from the knowledge of n and $\sigma(n)$. **[10]**

Solution: If $n = pq$, the only positive divisors of n are $1, p, q, pq$ and so $\sigma = \sigma(n) = 1 + p + q + pq$. We have $1 + p + \frac{n}{p} + n = \sigma$. Multiplying both sides with p we get a quadratic equation in p:

$$p^2 + p(1 + n - \sigma) + n = 0.$$

We know n, σ and so can solve for p in time polynomial in $\log_2 \sigma$. (Square roots can be computed in poly time.)

4. We have seen how to lift solutions to congruences of the form $f(x) \equiv 0 \pmod{p^e}$ to the solutions of $f(x) \equiv 0 \pmod{p^{e+1}}$.

   (a) Let $f(x)$ be a polynomial with integer coefficients, $e \in \mathbb{N}$ and z a solution of $f(x) \equiv 0 \pmod{p^e}$. Write $z' = z + kp^e$. Show how we can compute all values of k for which z' satisfies $f(z') \equiv 0 \pmod{p^{2e}}$. **[8]**

   Solution: Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$ for $0 \le i \le d$. Then $f'(x) = da_d x^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + 2a_2 x + a_1$. For $z' = z + kp^e$, we have

$$\begin{aligned} f(z') &= f(z + kp^e) \\ &= a_d(z + kp^e)^d + a_{d-1}(z + kp^e)^{d-1} + \cdots + a_1(z + kp^e) + a_0 \\ &= f(z) + kp^e(da_d z^{d-1} + (d-1)a_{d-1}z^{d-2} + \cdots + 2a_2 z + a_1) + p^{2e}g(z) \\ &= f(z) + kp^e f'(z) + p^{2e}g(z) \end{aligned}$$

   where $g(z)$ is some polynomial in z. Modulo p^{2e}, the above equation reduces to $f(z') \equiv f(z) + kp^e f'(z) \pmod{p^{2e}}$. We need to find values of k for which $f(z') \equiv \pmod{p^{2e}}$, which are given by solutions of

$$kp^e f'(z) \equiv -f(z) \pmod{p^{2e}}.$$

   Since $p^e | f(z)$, we can divide by p^e leading to the congruence

$$kf'(z) \equiv -\frac{f(z)}{p^e} \pmod{p^e}.$$

   (b) Given that the only solution to $2x^3 + 4x^2 + 3 \equiv 0 \pmod{25}$ is $14 \pmod{25}$, use the lifting procedure of Part (a) to compute all the solutions of $2x^3 + 4x^2 + 3 \equiv 0 \pmod{625}$. **[7]**

   Solution: Set $f(x) = 2x^3 + 4x^2 + 3$, $p = 5$ and $e = 2$ to apply the lifting procedure. We have $f'(x) = 6x^2 + 8x$ and it is given that $f(14) \equiv 0 \pmod{25}$. In order to find roots of $f(x)$ modulo 625, we need to solve for k in the following congruence: $kf'(z) \equiv -\frac{f(z)}{p^e} \pmod{p^e}$. We have $f'(z) = f'(14) = 1288 \equiv 13 \pmod{25}$ and $f(z)/p^e = 6275/25 = 251 \equiv 1 \pmod{25}$. We now need to solve the congruence $13k \equiv -1 \pmod{25}$. Multiplying by $13^{-1} = 2 \pmod{25}$ yields $k \equiv 2 \cdot (-1) \pmod{25}$ resulting in a unique solution for k given by $23 \pmod{25}$. Substituting for k, we get a unique solution $z + kp^e = 14 + 23 \cdot 25 \equiv 589 \pmod{625}$ for the congruence $f(x) \equiv 0 \pmod{625}$.

5. Let p be an odd prime and $e \in N$.

   (a) For $a, b \in \mathbb{Z}^*_{p^e}$, show that $a^2 \equiv b^2 \pmod{p^e}$ if and only if $a \equiv \pm b \pmod{p^e}$. **[9]**

Solution: Suppose $a^2 \equiv b^2 \pmod{p^e}$. Then $p^e|(a^2 - b^2)$ i.e., $p^e|(a+b)(a-b)$. It must be the case that $p^e|(a+b)$ or $p^e|(a-b)$. For otherwise, p divides both $a+b$ and $a-b$, implying that $p|2a$ which is impossible since $a \in \mathbb{Z}_{p^e}^*$ and p is odd. Hence, $a \equiv \pm b \pmod{p^e}$.

(b) Prove that $|\mathsf{QR}_{p^e}| = \phi(p^e)/2$.
(Here, QR_m denotes the set of quadratic residues modulo m). **[6]**

Solution: Let $a_1, a_2, \ldots, a_{\phi(p^e)}$ be the elements of $\mathbb{Z}_{p^e}^*$ arranged in increasing order so that $a_i \equiv p^e - a_j \pmod{p^e}$ for all $i \in [1, \phi(p^e)/2]$ and $j \in [\phi(p^e)/2+1, \phi(p^e)]$. We have $\mathsf{QR}_{p^e} = \{a_1^2, a_2^2, \ldots, a_{\phi(p^e)}^2\}$. From the previous part, we know that $a_i^2 \equiv a_j^2 \pmod{p^e}$ if and only if $a_i \equiv \pm a_j \pmod{p^e}$ for $i, j \in [1, \phi(p^e)]$ and so $|\mathsf{QR}_{p^e}| \leq p^e/2$. Clearly $a_i \not\equiv \pm a_j \pmod{p^e}$, thus implying that $a_i^2 \not\equiv a_j^2 \pmod{p^e}$ for $i \neq j$ and $i, j \leq \phi(p^e)/2$. In other words, the first $\phi(p^e)/2$ squares are distinct, implying that $|\mathsf{QR}_{p^e}| = p^e/2$.