CS60094: Computational Number Theory, Spring 2020

Class Test 1

CSE 119/120, 8 PM — 12th February, 2020
Duration = 1 hour — Total marks = 20

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 $n \geq 2$. **[6]**

   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 p be an odd prime. Show that $\sum_{\alpha \in \mathbb{Z}_p^*} \alpha = \sum_{\alpha \in \mathbb{Z}_p^*} \alpha^{-1} = 0 \pmod{p}$. **[4]**

   Solution: By Fermat's little theorem, for every $\alpha \in \mathbb{Z}_p^*$, $\alpha^{p-1} = 1 \pmod{p}$. In other words, the roots of $g(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$ are precisely the elements of $\mathbb{Z}_p^*$. The coefficients of $x^{p-2}, x^{p-3}, \ldots, x$ in $g(x)$ are all 0. In particular the coefficient of x^{p-2} is the sum of all roots of $g(x)$ i.e., $\sum_{\alpha \in \mathbb{Z}_p^*} \alpha$. We therefore have $\sum_{\alpha \in \mathbb{Z}_p^*} \alpha = 0$. Also, since the set $\{\alpha^{-1} \mid \alpha \in \mathbb{Z}_p^*\}$ is same as $\mathbb{Z}_p^*$, we have $\sum_{\alpha \in \mathbb{Z}_p^*} \alpha^{-1} = 0$.

   Alternatively, $\sum_{\alpha \in \mathbb{Z}_p^*} \alpha = 1 + 2 + \cdots + (p-1) = \frac{p(p-1)}{2} \equiv 0 \pmod{p}$ since $p - 1$ is even and hence divisible by 2.

3. Use Hensel lifting and Chinese remainder theorem to solve the following polynomial congruence.

$$x^3 + 11x + 21 \equiv 0 \pmod{189}$$

   [6]

Solution: Let $f(x) = x^3 + 11x + 21$. We have $f'(x) = 3x^2 + 11$. Our task is to find solutions for $f(x) \equiv 0 \pmod{189}$. Since 189 factors as $3^3 \times 7$, we will first find solutions for $f(x) \equiv 0 \pmod{3^3}$ and $f(x) \equiv 0 \pmod{7}$ and then use CRT to find solutions modulo 189. For the former, we use Hensel lifting.

Solutions of $f(x) \equiv 0 \pmod{3}$: We have $f(0) \equiv 21 \equiv 0 \pmod{3}$, $f(1) \equiv 33 \equiv 0 \pmod{3}$ and $f(2) \equiv 51 \equiv 0 \pmod{3}$. Thus the solutions modulo 3 are $0, 1, 2$.

Solutions of $f(x) \equiv 0 \pmod{3^2}$: We first lift the root $x \equiv 0 \pmod{3}$. We have $f(0) = 21, f'(0) = 11$. The congruence $f'(0)k \equiv -\frac{f(0)}{3} \pmod{3}$ is satisfied by $k \equiv 1 \pmod{3}$; the lifted root is hence $0 + 1 \cdot 3 \equiv 3 \pmod{9}$.

Let us now lift the root $x \equiv 1 \pmod{3}$. We have $f(1) = 33, f'(1) = 14$ and there is a unique solution to the congruence $f'(1)k \equiv -\frac{f(1)}{3} \pmod{3}$ given by $k \equiv 2 \pmod{3}$. Therefore the lifted root is $1 + 2 \cdot 3 \equiv 7 \pmod{9}$.

For lifting $x \equiv 2 \pmod{3}$, we compute $f(2) = 51, f'(2) = 23$. Solving the congruence $f'(2)k \equiv -\frac{f(2)}{3} \pmod{3}$ yields $k \equiv 2 \pmod{3}$ giving us the lifted root $2+2\cdot3 \equiv 8 \pmod{9}$.

Solutions of $f(x) \equiv 0 \pmod{3^3}$: The roots of $f(x)$ modulo 3^2 are $3, 7, 8$.

For lifting the first root $x \equiv 3 \pmod{3^2}$, compute $f(3) = 81, f'(3) = 38$. The congruence $f'(3)k \equiv -\frac{f(3)}{3^2} \pmod{3}$ has a unique solution given by $k \equiv 0 \pmod{3}$, thus resulting in $3 + 0 \cdot 3^2 \equiv 3 \pmod{27}$ as the lifted root.

Next, we have $f(7) = 441, f'(7) = 158$ and the congruence $f'(7)k \equiv -\frac{f(7)}{3^2} \pmod{3}$ has $k \equiv 1 \pmod{3}$ satisfying it. Thus the lifted root is $7 + 1 \cdot 3^2 \equiv 16 \pmod{27}$.

In order to lift $x \equiv 8 \pmod{3^2}$, we calculate $f(8) = 621, f'(8) = 203$ and look for solutions of the congruence $f'(8)k \equiv -\frac{f(8)}{3^2} \pmod{3}$. The congruence is satisfied by $k \equiv 0 \pmod{3}$ resulting in $8 \pmod{27}$ being the lifted root.

Summing up, the roots modulo 27 are 3,8,16.

Solutions of $f(x) \equiv 0 \pmod{7}$: We have $f(0) \equiv 21 \equiv 0 \pmod{7}$ and $f(i) \not\equiv 0 \pmod{7}$ for all $i \in \mathbb{Z}_7 \setminus \{0\}$. The only root of $f(x)$ modulo 7 is 0.

Solutions of $f(x) \equiv 0 \pmod{189}$: We finally use CRT to combine the roots of $f(x)$ modulo 27 and 7. We have $27^{-1} \equiv 6 \pmod{7}$ and $7^{-1} \equiv 4 \pmod{27}$. Therefore all solutions of $f(x) \equiv 0 \pmod{189}$ are of the form $a \times 7 \times 4 + b \times 27 \times 6 \pmod{189}$ where $a \in \{3, 8, 16\}$ and $b = 0$. The roots are precisely $84, 224 \equiv 35 \pmod{189}, 448 \equiv 70 \pmod{189}$.

4. Let p be an odd prime. Prove that the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$. **[4]**

Solution: $x^2 \equiv -1 \pmod{p}$ has a solution *iff* -1 is a quadratic residue modulo p *iff* $\left(\frac{-1}{p}\right) = 1$ *iff* $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ *iff* $(p-1)/2$ is even *iff* $2 \mid ((p-1)/2)$ *iff* $4 \mid (p-1)$ *iff* $p \equiv 1 \pmod{4}$.