CS60082 Computational Number Theory, Spring 2008

Mid-semester examination: Solutions

[*This test is open-notes. Answer all questions. Be brief and precise.*]

1 Compute all the simultaneous solutions of the following congruences. **(15)**

$$\begin{aligned} 5x &\equiv 3 \pmod{47}, \\ 3x^2 &\equiv 5 \pmod{49}. \end{aligned}$$

Solution We first solve $5x \equiv 3 \pmod{47}$. This requires computing $5^{-1} \times 3 \pmod{47}$. One may formally run the extended gcd algorithm on $5, 47$ to that effect. But, by simple inspection, one obtains $1 = 19 \times 5 + (-2) \times 47$, so $5^{-1} \equiv 19 \pmod{47}$, that is, the given congruence has the solution $x \equiv 19 \times 3 \pmod{47}$, that is, $\boxed{x \equiv 10 \pmod{47}}$.

Next we solve $3x^2 \equiv 5 \pmod{49}$. We have $49 = 7^2$, so we solve $3x^2 \equiv 5 \pmod 7$ first. This implies $x^2 \equiv 3^{-1} \times 5 \equiv 5 \times 5 \equiv 4 \pmod 7$. That is, $x \equiv 2, 5 \pmod 7$. Next, we lift these solutions to solutions modulo 49. We have $f(x) = 3x^2 - 5$, so that $f'(x) = 6x$. A lifted solution is $x_1 \equiv x_0 + 7t \pmod{49}$, where $x_0 = 2, 5$ and $f'(x_0)t \equiv -\frac{f(x_0)}{7} \pmod 7$. For $x_0 = 2$, we have $12t \equiv -1 \pmod 7$, that is, $t \equiv 4 \pmod 7$, so that $x_1 \equiv 2 + 4 \times 7 \equiv 30 \pmod{49}$. For $x_0 = 5$, we have $30t \equiv -10 \pmod 7$, that is, $t \equiv 2 \pmod 7$, so that $x_1 \equiv 5 + 2 \times 7 \equiv 19 \pmod{49}$. Thus, the two solutions of $3x^2 \equiv 5 \pmod{49}$ are $\boxed{x \equiv 19, 30 \pmod{49}}$.

Finally, we combine the solutions by the CRT. We have $24 \times 47 + (-23) \times 49 = 1$, that is, $49^{-1} \equiv -23 \equiv 24 \pmod{47}$ and $47^{-1} \equiv 24 \pmod{49}$. Thus, by CRT, the simultaneous solutions are $x \equiv 24 \times 49 \times a + 24 \times 47 \times b \pmod{47 \times 49}$, where $a = 10$ and $b = 19, 30$. Plugging in the values gives $\boxed{x \equiv 950, 1843 \pmod{2303}}$.

2 Let $\sigma(n)$ denote the sum of positive integral divisors of $n \in \mathbb{N}$. 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 We have $\sigma(pq) = 1 + p + q + pq = 1 + p + q + n$. If n and $\sigma(n)$ are provided, we obtain pq and $p + q$. Finally, p, q can be obtained by solving a quadratic equation.

3 Let $n = pq$ be a product of two distinct *known* primes p, q. Assume that $q^{-1} \pmod p$ is available.

Suppose we want to compute $b \equiv a^e \pmod n$ for $a \in \mathbb{Z}_n^*$ and $0 \leqslant e < \phi(n)$. To that effect, we first compute $e_p = e \text{ rem } (p-1)$ and $e_q = e \text{ rem } (q-1)$ and then the modular exponentiations $b_p \equiv a^{e_p} \pmod p$ and $b_q \equiv a^{e_q} \pmod q$. Finally, compute $t \equiv q^{-1}(b_p - b_q) \pmod p$.

(a) Prove that $b \equiv b_q + tq \pmod n$. **(10)**

Solution We have $b_p \equiv b \pmod p$ and $b_q \equiv b \pmod q$, so we have to combine these two values by the CRT. Let $\beta = b_q + tq$. Then, $\beta \equiv b_q \pmod q$. Also, $tq \equiv b_p - b_q \pmod p$, so $\beta \equiv b_q + (b_p - b_q) \equiv b_p \pmod p$. Therefore, $\beta \equiv b \pmod{pq}$.

(b) Suppose that p, q are both of bit sizes roughly half of that of n. Explain how computing b in this method speeds up the exponentiation process. You may assume classical (that is, high-school) arithmetic for the implementation of products and Euclidean division. **(5)**

Solution Let $s = |n|$ be the bit size of n. We than have the bit sizes $|p| \approx s/2$ and $|q| \approx s/2$. Since modular exponentiation is done in cubic time, computing the two modular exponentiations to obtain b_p and b_q takes a total time which is about $1/4$-th that of computing $b \equiv a^e \pmod n$ directly. The remaining operations in the modified algorithm can be done in $\mathrm{O}(s^2)$ time. Thus, we get a speed-up of about 4.

4 Imitate the binary gcd algorithm in order to compute the Jacobi symbol $\left(\frac{a}{b}\right)$. **(10)**

Solution Since we can extract powers of 2 easily from a, we assume that a is odd. For the Jacobi symbol, b is odd too. If $a = b$, then $\left(\frac{a}{b}\right) = 0$. If $a < b$, we use the quadratic reciprocity law to write $\left(\frac{a}{b}\right)$ in terms of $\left(\frac{b}{a}\right)$. So it remains only to analyze the case of $\left(\frac{a}{b}\right)$ with a, b odd and $a > b$. Let $\alpha = a - b$. We write $\alpha = 2^r a'$ with $r \in \mathbb{N}$ and a' odd. If r is even, then $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$, whereas if r is odd, then $\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)\left(\frac{a'}{b}\right) = (-1)^{(b^2-1)/8}\left(\frac{a'}{b}\right)$. So, the problem reduces to computing $\left(\frac{a'}{b}\right)$ with both a', b odd.

5 (a) Compute the continued fraction expansion of $\sqrt{5}$. **(5)**

Solution

$$\begin{aligned}
\xi_0 &= \sqrt{5} = 2.236\ldots, & a_0 &= \lfloor \xi_0 \rfloor = 2 \\
\xi_1 = \frac{1}{\xi_0 - a_0} = \frac{1}{\sqrt{5}-2} &= \sqrt{5} + 2 = 4.236\ldots, & a_1 &= \lfloor \xi_1 \rfloor = 4 \\
\xi_2 = \frac{1}{\xi_1 - a_1} = \frac{1}{\sqrt{5}-2} &= \sqrt{5} + 2 = 4.236\ldots, & a_2 &= \lfloor \xi_2 \rfloor = 4 \\
& \ldots
\end{aligned}$$

Thus, $\sqrt{5} = \langle 2, 4, 4, 4, \ldots \rangle = \langle 2, \overline{4} \rangle$.

(b) It is known that all the solutions of $x^2 - 5y^2 = 1$ with $x, y > 0$ are of the form $x = h_n$ and $y = k_n$, where h_n/k_n is a convergent to $\sqrt{5}$. Find the solution of $x^2 - 5y^2 = 1$ with the smallest possible $y > 0$. **(5)**

Solution The first convergent is $r_0 = \frac{h_0}{k_0} = \langle 2 \rangle = 2/1$, that is, $h_0 = 2$ and $k_0 = 1$. But $h_0^2 - 5k_0^2 = -1$. Then, we have $r_1 = \frac{h_1}{k_1} = \langle 2, 4 \rangle = 2 + \frac{1}{4} = \frac{9}{4}$, that is, $h_1 = 9$ and $k_1 = 4$. We have $h_1^2 - 5k_1^2 = 1$. Since $k_0 \leqslant k_1 < k_2 < k_3 < \cdots$, the smallest solution is $(9, 4)$.

(c) Let (a, b) denote the smallest solution obtained in Part (b). Define the sequence of pairs (x_n, y_n) of positive integers recursively as follows.

$$\begin{aligned}
(x_0, y_0) &= (a, b) \text{ and} \\
(x_n, y_n) &= (ax_{n-1} + 5by_{n-1}, bx_{n-1} + ay_{n-1}) \text{ for } n \geqslant 1.
\end{aligned}$$

Prove that each (x_n, y_n) is a solution of $x^2 - 5y^2 = 1$. (In particular, there are infinitely many solutions in positive integers of the *Pell equation* $x^2 - 5y^2 = 1$.) **(5)**

Solution We proceed by induction on n. For $n = 0$, $(x_0, y_0) = (a, b) = (9, 4)$ is a solution of $x^2 - 5y^2 = 1$ by Part (b). So assume that $n \geqslant 1$ and that $x_{n-1}^2 - 5y_{n-1}^2 = 1$. But then

$$\begin{aligned}
x_n^2 - 5y_n^2 &= (ax_{n-1} + 5by_{n-1})^2 - 5(bx_{n-1} + ay_{n-1})^2 \\
&= a^2(x_{n-1}^2 - 5y_{n-1}^2) - 5b^2(x_{n-1}^2 - 5y_{n-1}^2) \\
&= a^2 - 5b^2 = 1.
\end{aligned}$$