CS60082/CS60094 Computational Number Theory, Spring 2010–11

Mid-Semester Test

Maximum marks: 30 | Date: February 2011 | Duration: 2 hours

Roll no: ________________ **Name:** ____

[*Write your answers in the question paper itself. Be brief and precise. Answer all questions.*]

1. (a) Let $n = p^2q$ with p, q distinct odd primes, $p \nmid (q-1)$ and $q \nmid (p-1)$. Prove that factoring n is polynomial-time equivalent to computing $\phi(n)$. **(3)**

Solution We have $n = p^2q$ and $\phi(n) = p(p-1)(q-1)$. If p, q are known, we can compute $\phi(n)$ in polynomial time. Conversely, if $\phi(n)$ is known, we compute $p = \gcd(n, \phi(n))$ and obtain $q = n/p^2$.

(b) Let $n = p^2q$ with p, q odd primes satisfying $q = 2p + 1$. Argue that one can factor n in polynomial time. **(3)**

Solution Substituting $q = 2p + 1$ gives $p^2(2p + 1) - n = 0$, a cubic equation in the variable p. One can use a standard numerical method (like the Newton-Raphson method) to solve for p. One may use integer calculations only. If one chooses to use floating-point calculations instead, one should work with a precision of $\Theta(\log n)$ bits.

2. Let a, b, c be non-zero integers, and $d = \gcd(a, b)$.

(a) Prove that the equation

$$ax + by = c \qquad (*)$$

is solvable in *integer values* of x, y if and only if $d \mid c$. **(3)**

Solution [If] By Bézout's theorem, $au + bv = d$ for some integers u, v. Let $c = ld$. But then $a(lu) + b(lv) = c$, that is, Eqn $(*)$ has a solution (lu, lv).

[Only if] If (s, t) is a solution of Eqn $(*)$, then $as + bt = c$. Now, d divides both a and b, that is, $as + bt$ too, that is, $d \mid c$.

(b) Suppose that $d \mid c$, and (s, t) is a solution of Eqn $(*)$. Prove that all the solutions of Eqn $(*)$ can be given as $(s + k(b/d), t - k(a/d))$ for all $k \in \mathbb{Z}$. Describe how one solution (s, t) can be efficiently computed. **(3)**

Solution If (s', t') is another solution of Eqn $(*)$, we have $as + bt = c = as' + bt'$, that is, $(a/d)(s' - s) = (b/d)(t - t')$. But $\gcd(a/d, b/d) = 1$, so $(b/d) \mid (s' - s)$, that is, $s' - s = k(b/d)$ for some $k \in \mathbb{Z}$. But then $t - t' = k(a/d)$. Therefore, it suffices to determine one solution (s, t) of Eqn $(*)$. By an extended gcd algorithm, compute u, v such that $au + bv = d$. Compute $l = c/d = c/\gcd(a.b)$. Take $s = lu$ and $t = lv$.

(c) Compute all the (integer) solutions of the equation $21x + 15y = 60$. **(3)**

Solution We have $\gcd(21, 15) = 3 = 21 \times 3 + 15 \times (-4)$, so $60 = 20 \times 3 = 21 \times 60 + 15 \times (-80)$, that is, all the solutions of $21x + 15y = 60$ are $(60 + k(15/3), -80 - k(21/3)) = (60 + 5k, -80 - 7k)$ for all $k \in \mathbb{Z}$.

3. Let p be an odd prime, $a \in \mathbb{Z}_p^*$, and $e \in \mathbb{N}$. Prove that the multiplicative order of $1 + ap$ modulo p^e is p^{e-1}. (**Remark:** This result can be used to obtain primitive roots modulo p^e.) **(6)**

Solution The result being obvious for $e = 1$, take $e \geqslant 2$. Let me first prove the following important result.

Lemma: For every $e \geqslant 2$, we have $(1 + ap)^{P^{e-2}} \equiv 1 + ap^{e-1} \pmod{p^e}$.

Proof We proceed by induction on e. For $e = 2$, both sides of the congruence are equal to the integer $1 + ap$. So assume that the given congruence holds for some $e \geqslant 2$. We investigate the value of $(1 + ap)^{p^{e-1}}$ modulo p^{e+1}. By the induction hypothesis, $(1 + ap)^{p^{e-2}} = 1 + ap^{e-1} + up^e$ for some integer u. Raising both sides of this equality to the p-th power gives

$$\begin{aligned}(1+ap)^{p^{e-1}} &= (1 + ap^{e-1} + up^e)^p \\ &= 1 + \binom{p}{1}(ap^{e-1} + up^e) + \binom{p}{2}(ap^{e-1} + up^e)^2 + \cdots + \\ &\quad \binom{p}{p-1}(ap^{e-1} + up^e)^{p-1} + (ap^{e-1} + up^e)^p \\ &= 1 + ap^e + p^{e+1} \times v\end{aligned}$$

for some integer v (since p is prime so that $p|\binom{p}{k}$ for $1 \leqslant k \leqslant p-1$, and since the last term in the binomial expansion is divisible by $p^{p(e-1)}$, in which the exponent $p(e-1) \geqslant e+1$ for all $p \geqslant 3$ and $e \geqslant 2$). This completes the proof of the lemma.

Let us now derive the order of $1 + ap$ modulo p^e. Using the lemma for $e + 1$ indicates $(1 + ap)^{p^{e-1}} \equiv 1 + ap^e \pmod{p^{e+1}}$ and, in particular, $(1 + ap)^{p^{e-1}} \equiv 1 \pmod{p^e}$. Therefore, $\operatorname{ord}_{p^e}(1 + ap) \mid p^{e-1}$. The lemma also implies that $(1 + ap)^{p^{e-2}} \not\equiv 1 \pmod{p^e}$ (for a is coprime to p), that is, $\operatorname{ord}_{p^e}(1 + ap) \nmid p^{e-2}$. We, therefore, have $\operatorname{ord}_{p^e}(1 + ap) = p^{e-1}$.

4. (a) Which of the polynomials $x^2 \pm 7$ is irreducible modulo 19? Justify. **(3)**

Solution Since $\left(\frac{7}{19}\right) = (-1)^{(7-1)(19-1)/4}\left(\frac{19}{7}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) = -(-1)^{(5-1)(7-1)/4}\left(\frac{7}{5}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = -(-1) = +1$, we conclude that 7 is a quadratic residue modulo 19. But $19 \equiv 3 \pmod 4$, so -7 is a quadratic non-residue modulo 19. Thus, $x^2 - 7$ is reducible modulo 19, whereas $x^2 + 7$ is irreducible modulo 19.

(b) Using the irreducible polynomial $f(x)$ of Part (a), represent the finite field $\mathbb{F}_{361} = \mathbb{F}_{19^2}$ as $\mathbb{F}_{19}(\theta)$, where $f(\theta) = 0$. Compute $(2\theta + 3)^{11}$ in this representation of $\mathbb{F}_{361}$ using the left-to-right square-and-multiply exponentiation algorithm. Show your calculations. **(6)**

Solution We take $f(x) = x^2 + 7$, that is, $\theta^2 + 7 = 0$, that is, $\theta^2 = -7 = 12$. The binary expansion of 11 is $(1011)_2$. Therefore, the left-to-right exponentiation proceeds as follows. The variable "Product" is initialized to 1.

Bit	Operation	Product
1	Sqr	1
	Mul	$2\theta + 3$
0	Sqr	$(2\theta + 3)^2 = 4\theta^2 + 12\theta + 9 = 4 \times 12 + 12\theta + 9 = 12\theta$
1	Sqr	$(12\theta)^2 = 144 \times \theta^2 = 11 \times 12 = 18$
	Mul	$18 \times (2\theta + 3) = 17\theta + 16$
1	Sqr	$(17\theta + 16)^2 = 289\theta^2 + 544\theta + 256 = 4 \times 12 + 12\theta + 9 = 12\theta$
	Mul	$(12\theta)(2\theta + 3) = 24\theta^2 + 36\theta = 5 \times 12 + 17\theta = 17\theta + 3$

We conclude that $(2\theta + 3)^{11} = 17\theta + 3$.