

# CS5610: Final Exam

Total Marks: 35

1. Find integers  $x, y$  such that  $12x + 17y = 1$ . [2 marks]
2. Find all primes  $p$  such that  $(p - 3)! \equiv 7 \pmod{p}$ . [2 marks]
3. Let  $n = 450$  and let  $f(x) \in \mathbb{Z}_n[x]$  be a non-zero polynomial of degree 3 with  $d$  distinct roots. What are the possible values of  $d$ ? [2 marks]
4. Let  $p$  be an odd prime and  $r \in \{1, 2, \dots, p - 1\}$ . Show that there is a positive integer  $n$  such that  $n^n - r$  is divisible by  $p$ . [3 marks]
5. Find  $f(x) \in \mathbb{Z}_7[x]$  such that  $f(x)(2x + 1) \equiv 1 \pmod{x^2 + 1}$ . [3 marks]
6. For each congruence below, decide whether it has a solution.
  - (a)  $x^2 \equiv 17 \pmod{101}$ .
  - (b)  $x^3 \equiv 5 \pmod{23}$ .
  - (c)  $x^3 \equiv 5 \pmod{31}$ .[3 marks]
7. Let  $p$  be an odd prime.
  - (a) Show that if  $x^n - 1$  is divisible by  $x^k - 1$  in  $\mathbb{Z}_p[x]$ , then  $k$  must divide  $n$ . [2 marks]
  - (b) Let  $f(x) = 1 + x + x^2 + \dots + x^r$ , where  $r \leq p - 1$ . Show that if  $f(x)$  is irreducible in  $\mathbb{Z}_p[x]$ , then  $(r + 1)$  must divide  $p^r - 1$ . [2 marks]
8. Let  $p$  be an odd prime and let  $n = 2p + 1$ . Suppose that  $2^p \equiv 1 \pmod{n}$ . Show that  $n$  is prime. [4 marks]
9. Suppose that we modify Dixon's algorithm in the following way: instead of computing  $b_1, \dots, b_m$  as  $b_i = a_i^2 \pmod{n}$ , we compute  $b_i = a_i^3 \pmod{n}$  and try find a relation of the form  $\alpha^3 \equiv \beta^3 \pmod{n}$ . Subsequently, as in Dixon's algorithm, we find  $\gcd(\alpha - \beta, n)$  as a potential factor of  $n$ .
  - (a) Explain what modification should be made to the rest of the algorithm to find such  $\alpha, \beta$ . [2 marks]
  - (b) For which values of  $n$  can this modified idea still work to find a factor and for which values of  $n$  will this modification never produce any factors? [4 marks]

10. In the AKS primality test, we needed to test the identity:

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}$$

for various values of  $a$ .

Suppose that we know  $r \in \mathbb{N}$  and  $\alpha, \beta \in \mathbb{Z}_n$  such that

- (a)  $r > 4 \log^2 n$  and  $r$  divides  $(n - 1)$ .
- (b)  $x^r - \alpha$  is irreducible modulo  $p$  for some prime divisor  $p$  of  $n$ ;
- (c)  $\beta$  is a primitive  $r$ th root of unity in  $\mathbb{Z}_n$ .

Then show via the following exercises that the single test:

$$(x + 1)^n = x^n + 1 \pmod{n, x^r - \alpha}$$

is sufficient to test whether  $n$  is prime, assuming that  $n$  is not a perfect power.

We will suppose for contradiction that  $n$  is composite.

- (a) Show that for every  $0 \leq i \leq r$ , the pairs  $(n, \beta^i x + 1)$  are introspective, i.e.  $(\beta^i x + 1)^n \equiv (\beta^i x)^n + 1 \pmod{x^r - \alpha, p}$ . **[2 marks]**
- (b) As in the original algorithm, let  $I = \{n^i p^j | i, j \geq 0\}$ . Let  $\mathbb{F} = \mathbb{Z}_p[x]/(x^r - \alpha)$ . Find a subgroup  $R$  of  $\mathbb{F}^*$  such that  $|R| \geq 2^r$  and  $(m, f(x))$  is introspective for every  $m \in I, f(x) \in R$ . **[2 marks]**
- (c) Let  $G$  be the multiplicative subgroup of  $\mathbb{Z}_r^*$  generated by  $n$  and  $p$ , and let  $t = |G|$ . As in the AKS algorithm, we may deduce that  $|R| \leq n^{2\sqrt{t}}$  (you don't have to show this). Combine this with the lower bound on  $|R|$  to obtain a contradiction. **[2 marks]**