

Due: Monday December 5th, 1pm.

1) 14.6.5

2) 14.6.9

3) 14.6.11

4) Suppose  $k < n$ . A  $k \times n$  Latin rectangle is a table with  $k$  rows and  $n$  columns, such that the symbols  $1, 2, \dots, n$  appear exactly once in each row and at most once in each column. Show that a  $k \times n$  Latin rectangle can be extended to  $n \times n$  Latin square.

5) Let  $C$  be a  $t$ -error-correcting binary code of length  $n$ . Show that

$$(i) \quad |C| \leq \frac{2^n}{\sum_{i=0}^t \binom{n}{i}} \quad \text{and} \quad (ii) \quad |C| \leq 2^{n-2t}.$$

6) Let  $p$  be a prime and let  $\mathbb{F}_p$  be the field of order  $p$ , i.e. the set of all residues modulo  $p$ . Show that there is a *multiplicative generator*, i.e. an element  $a \in \mathbb{F}_p$  so that  $a, a^2, a^3, \dots, a^{p-1}$  is a complete list of the elements of  $\mathbb{F}_p$ . Deduce that primality is an NP property.

(Hint: For  $x \in \mathbb{F}_p$  define its order as  $o(x) = \min\{t : t \geq 1, x^t = 1\}$ . Choose  $a$  so that  $o(a)$  is as large as possible. Show that  $o(x)|o(a)$  for any  $x \in \mathbb{F}_p$ , and deduce that  $o(a) = p - 1$ .)

7) Suppose  $p = 6t + 1$  for some integer  $t$ . Let  $B_{i,x} = \{a^i + x, a^{2t+i} + x, a^{4t+i} + x\}$  for  $0 \leq i < t$  and  $x \in \mathbb{F}_p$ , where  $a$  is a multiplicative generator for  $\mathbb{F}_p$  (given by question 6). Show that the collection of all blocks  $B_{i,x}$  gives a Steiner Triple System on the set  $\mathbb{F}_p$ .

8) Suppose that  $p$  is a prime and  $a$  is a multiplicative generator for  $\mathbb{F}_p$ . Suppose that that it is computationally unfeasible to solve the equation  $a^x = y$  when  $y$  is given but  $x$  is to be determined (although given  $x$  it is quick to compute  $y$ ). Alice and Bob communicate by sending each other elements of  $\mathbb{F}_p$ , but these communications are open to the public. Describe a method by which they can agree on an element of  $\mathbb{F}_p$  in such a way that it is computationally unfeasible for an observer to determine what that element is.