

## MATH 145, SAMPLE PROBLEMS FOR EXAM 1, 08 FEB, 2008

(Here is a sampling of problems that may be included in Friday's exam. In order to get the most out of them, hide the solutions until you have worked the problems yourself.)

- (1) Two standard cubical dice, one red and one green, are rolled. What is the number of possible outcomes? What is the number of possible outcomes where the sum of the spots showing is either 7 or 11?

There are six faces on each die; for each red outcome, there are six green outcomes. Hence the total number of outcomes is  $6^2 = 36$ . Each outcome can be represented as a pair  $(m, n)$ , where  $1 \leq m \leq 6$  is the number of red spots and  $1 \leq n \leq 6$  is the number of green spots.  $m + n = 7$  has 6 distinct solutions, and  $m + n = 11$  has two more. So the total number of outcomes here is 8.

- (2) In a chess tournament with 50 participants, officials plan the first round of play by choosing 25 separate pairs of players. In how many ways can this be done, noting that it matters who plays white and who plays black?

If the order in which the pairs of players were chosen mattered, then the number would be  $P(50, 2)P(48, 2) \dots P(2, 2)$ . But this order doesn't matter, so the number is actually  $\frac{1}{25!}P(50, 2)P(48, 2) \dots P(2, 2) = \frac{50!}{25!}$ .

- (3) Suppose set  $A$  has 3 elements and set  $B$  has 5 elements. How many functions from  $A$  to  $B$  are there? How many of them are one-one? How many are onto?

The first element has five possible choices, as does the second, as does the third. So the total number of functions is  $5^3 = 125$ . When constructing a one-one function, the first element has five possible choices; but once that has been chosen, there are only four choices for the second, and then only three choices for the third. So the number of one-one functions is  $P(5, 3) = 60$ . There are no onto functions because the range is too big.

- (4) In the binomial expansion of  $(x + y)^{25}$ , what is the coefficient of  $x^4y^{21}$ ?

It's just  $C(25, 4) = \frac{25!}{4!21!} = 11,400$ .

- (5) How many equivalence relations are there on a nine-element set, if each equivalence class has three elements?

Because equivalence relations are paired up with partitions, this is the number of partitions of a nine-element set into three-element blocks. This number is  $\frac{1}{3!}C(9, 3)C(6, 3)C(3, 3) = \frac{9!}{(3!)^4} = 280$

- (6) What are  $(28) \bmod 15$ ,  $(-40) \bmod 7$ ,  $(9^{100}) \bmod 7$ ?

$28 = 15(1) + 13$ , so  $(28) \bmod 15 = 13$ .  $-40 = 7(-6) + 2$ , so  $(-40) \bmod 7 = 2$ . Since  $(9) \bmod 7 = 2$ ,  $(9^{100}) \bmod 7 = (2^{100}) \bmod 7 = (2^{3 \cdot 33 + 1}) \bmod 7 = (8^{33} \cdot 2) \bmod 7 = (1^{33} \cdot 2) \bmod 7 = (2) \bmod 7 = 2$ .

(7) Solve the equation  $x^2 + 2 = 0$  in  $\mathbb{Z}_6$ .

We're looking for all  $a \in \mathbb{Z}_6$  so that  $a^2 = (-2) \bmod 6 = 4$ . By squaring all the integers  $0 \leq n \leq 5$  and reducing modulo 6, we get the solutions  $x = 2$  and  $x = 4$ .

(8) Find  $\gcd(375, 180)$  using the Euclidean GCD algorithm.

Because  $375 = 180(2) + 15$ , we have  $\gcd(375, 180) = \gcd(180, 15) = \gcd(15, 0) = 15$ .

(9) Does  $(8^{-1}) \bmod 12$  exist? If so, what is it; if not, why not.

An element  $a \in \mathbb{Z}_N$  exists—i.e.,  $a$  is a unit of  $\mathbb{Z}_N$ —iff  $\gcd(a, N) = 1$ . But  $\gcd(8, 12) = 4$ ; hence 8 is not a unit of  $\mathbb{Z}_{12}$ .

(10) If  $p$  is a prime number, how many units does  $\mathbb{Z}_p$  have?

Every integer from 1 to  $p - 1$  is relatively prime to  $p$ ; hence there are  $p - 1$  units in  $\mathbb{Z}_p$ .

(11) If  $p$  and  $q$  are two different prime numbers, how many units does  $\mathbb{Z}_{pq}$  have?

It's easier to count the *non*-units. First off, there's 0; then there are the multiples of  $p$  less than  $pq$  ( $q - 1$  of these); in addition to that there are the multiples of  $q$  less than  $pq$  ( $p - 1$  of these). Hence there are  $p + q - 1$  nonunits in  $\mathbb{Z}_{pq}$ , leaving  $pq - (p + q - 1)$  units.

(12) Given that  $6 \cdot 151 - 5 \cdot 181 = 1$  find  $(6^{-1}) \bmod 5$ ,  $(6^{-1}) \bmod 181$ , and  $(5^{-1}) \bmod 151$ .

$(6^{-1}) \bmod 5 = (151) \bmod 5 = 1$ ; and  $(6^{-1}) \bmod 181 = 151$ . Finally, rewriting the given equality as  $5 \cdot (-181) + 6 \cdot 151 = 1$ , we have  $(5^{-1}) \bmod 151 = (-181) \bmod 151 = 151 - (181) \bmod 151 = 151 - 30 = 121$ .

(13) Show by example (i.e., by picking  $N$  and  $a, b \in \mathbb{Z}_N$ ) that the equation  $ax = b$  can have exactly two solutions modulo  $N$ .

Pick  $N = 6$ ,  $a = 2$ ,  $b = 0$ . Then the two solutions to  $2x = 0$  in  $\mathbb{Z}_6$  are  $x = 0$  and  $x = 3$ .