MATH 240: Discrete structures I. Fall 2011

Assignment #4: Cryptography and combinatorics. Solutions.

1. *Fermat primality test.*
A number m passes the Fermat primality test if $2^{m-1} \equiv 1 (\mathrm{mod}\, m)$.

a) Does m = 2047 pass the test?

b) Did the test give the correct answer in this case?

Solution a): Yes. $2047 = 2^{11} - 1$.

$$2^{2047-1} = 2^{2046} = 2^{11 \cdot 186} = (2^{11})^{186} \equiv 1 (\mathrm{mod}\, 2047).$$

b) No. $2047 = 23 \cdot 89$.

2. *RSA encryption.* Using a public key $N = 55$ and an exponent $e = 3$ we want to transmit a message $m = 12$.

a) What is the encryption $m^*$of m using RSA?

b) Run the RSA decryption method to decrypt m^*.

Solution a):

$$\begin{aligned} m^* &\equiv 12^3 (\mathrm{mod}\, 55) \\ 12^2 &= 144 = 110 + 34 \equiv 34 (\mathrm{mod}\, 55) \\ 12^3 &\equiv 34 \cdot 12 = 408 = 7 \cdot 55 + 23 \equiv 23 (\mathrm{mod}\, 55) \\ m^* &= 23 \end{aligned}$$

b): $p = 5, q = 11$. We need to find k such that $3k \equiv 1 (\mathrm{mod}(5-1)(11-1) = 40)$. $3 \cdot 27 = 81$, so $k = 27$ works. Finally, we compute $23^{27} (\mathrm{mod}\, 55)$.

$$\begin{aligned} 23^2 &= 729 = 9 \cdot 55 + 34 \equiv 34 (\mathrm{mod}\, 55) \\ 23^4 &\equiv 34^2 = 21 * 55 + 1 \equiv 1 (\mathrm{mod}\, 55) \\ 23^{27} &= 23^2 4 \cdot 23^3 \equiv 23^3 \equiv 34 \cdot 23 = 14 \cdot 55 + 12 \equiv 12 (\mathrm{mod}\, 55) \end{aligned}$$

3. *Bijection.* Give a bijection between the set of all integers and the set of all positive integers.

Solution: Let

$$f(k) = \begin{cases} 2k+1, & \text{if } k \geq 0, \\ 2|k|, & \text{if } k < 0. \end{cases}$$

It is easy to verify that f is a bijection from the integers to the positive integers.

4. *Counting techniques.* How many ways are there to position two black rooks and two white rooks on an 8×8 chessboard so that no two pieces of different colors share a row or a column

Solution: There are $64 \cdot 49/2$ ways two position two black rooks so that they don't share a row or a column and $64 \cdot 14/2$ ways to position them in the same row or in the same column. In the first case there are six rows and six columns which remain available for the white rooks and so there are $36 \cdot 35/2$ ways to position them, giving $64 \cdot 49 \cdot 36 \cdot 35/4$ ways. In the second case there are $64 \cdot 14 \cdot 42 \cdot 41/4$ ways. The total number is

$$\frac{64}{4}(49 \cdot 36 \cdot 35 + 14 \cdot 42 \cdot 41) = 1373568.$$

5. *Binomial coefficients.*

a) What is the coefficient of x^7y^5 in $(x+y)^{12}$?

(b) What is the coefficient of x^7y^5 in $(2x-y)^{12}$?

Solution: a)

$$\binom{12}{7} = \frac{12!}{7!5!} = 792.$$

b):

$$\binom{12}{7} 2^7(-1)^5 = -792 \cdot 128 = -101376.$$

6. *Combinatorial identity.*

a) Using the formula for binomial coefficients prove that for all positive integers $k \leq r \leq n$

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}.$$

(b) Give a bijective proof of the above formula by interpreting both sides as enumerating certain pairs of subsets of an n-element set.

Solution: a)

$$\binom{n}{r}\binom{r}{k} = \frac{n!}{r!(n-r)!} \cdot \frac{r!}{k!(r-k)!} = \frac{n!}{k!(r-k)!(n-r)!}$$
$$= \frac{n!}{k!(n-k)!} \cdot \frac{(n-k)!}{(r-k)!((n-k)-(r-k))!} = \binom{n}{k}\binom{n-k}{r-k}.$$

b): Denote $\{1, 2, \ldots, n\}$ by $[n]$. The left side of the formula enumerates the set

$$S = \{(A, B) \ : \ B \subseteq A \subseteq [n], |A| = r, |B| = k\},$$

while the right side enumerates the set

$$T = \{(C, D) \ : \ C, D \subseteq [n], C \cap D = \emptyset, |C| = k, |D| = r - k\}.$$

The function $f : S \to T$ such that $f(A, B) = (B, A - B)$ is a bijection, showing that $|S| = |T|$.