THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 **Exercises and Solutions for Week 8** 2004

1. Let $n = p_1^{n_1} \cdots p_t^{n_t}$ be an odd composite number, and for each i write $p_i - 1 = 2^{k_i} r_i$ with each r_i an odd number. Justify the probabilities

$$P(x^{2^j r} = -1) = \frac{1}{m} \prod_{i=1}^{t} \frac{1}{2^{k_i - j}}$$

where $x \in \mathbb{Z}/n\mathbb{Z}^*$ (chosen uniformly at random), $j < k_i$, and where m is the largest odd divisor of $|(\mathbb{Z}/n\mathbb{Z}^*)^r|$ for any odd number r.

Solution The value m is the odd part of the size of the subgroup $|(\mathbb{Z}/n\mathbb{Z}^*)^{2^j r}|$ of r-th multiples in $\mathbb{Z}/n\mathbb{Z}^*$, and the factor $2^{k_i - j}$ order of the even part in each component $\mathbb{Z}/p_i^{n_i}\mathbb{Z}^*$. When -1 is contained in the group, then the probability of $x^{2^j r}$ equalling -1 is the reciprocal of the order of $|(\mathbb{Z}/n\mathbb{Z}^*)^{2^j r}|$.

2. Recall the Miller–Rabin primality test:

```
1. let n − 1 = 2^s r for r odd
2. choose a at random in Z/nZ* and set u = a^r
3. if u = ±1 then return probable prime
4. for i in [1, ..., s − 1] {
        set u = u^2
        if u = −1 then
            return probable prime
        if u = +1 then
            return composite
   }
5. return composite
```

and explain why the sum

$$P(x^r = 1) + P(x^r = -1) + P(x^{2r} = -1) + \cdots + P(x^{2^{s-1} r} = -1)$$

gives the probability that the output is *probable prime*.

Solution The sum is over a disjoint set of events defining the conditions under which *probable prime* is returned.

3. For each of the following integers $15 = 3 \cdot 5$, $21 = 3 \cdot 7$, 29, $85 = 5 \cdot 17$, $105 = 3 \cdot 5 \cdot 7$, and $357 = 13 \cdot 29$, determine the probability that the Miller–Rabin primality test returns *probable prime*.

Solution Applying the formula at top, the values of r and $k_1, \dots, k_t$ give the probablities P in the table below.

n	r	$k_1, \dots, k_t$	P	
15	1	$1, 2$	$1/4$	$= 1/8 + 1/8$
21	3	$1, 1$	$1/6$	$= 1/12 + 1/12$
29	1	2	1	$= 1/4 + 1/4 + 1/2$
85	1	$2, 4$	$3/32$	$= 1/64 + 1/64 + 1/16$
105	3	$1, 2, 1$	$1/24$	$= 1/48 + 1/48$
377	21	$2, 2$	$1/56$	$= 1/336 + 1/336 + 1/84$

Note that r is computed as the odd part of $\varphi(n)/\mathrm{GCD}(n-1, \varphi(n))$.

4. Explain what happens when $j \geq k_i$ for some i, and demonstrate this with one of the above integers.

Solution When $j \geq k_i$ for some i, the element -1 is not in $[2^j](\mathbb{Z}/p_i\mathbb{Z}^*)$, hence not in $[2^j m](\mathbb{Z}/p_i\mathbb{Z}^*)$. Consequently, -1 can not be in $[2^j m](\mathbb{Z}/n\mathbb{Z}^*)$. Take for example $n = 15$, for which the k_i's are 1 and 2. While $[7](\mathbb{Z}/15\mathbb{Z}^*) = \mathbb{Z}/15\mathbb{Z}^*$, once we take squares, we see that $[2](\mathbb{Z}/15\mathbb{Z}^*)$ does not contain -1, since its image $[2](\mathbb{Z}/3\mathbb{Z}^*)$ does not contain -1 even though $[2](\mathbb{Z}/5\mathbb{Z}^*)$ does. We can verify that 1 and 4 are the only elements of $[2](\mathbb{Z}/15\mathbb{Z}^*)$, and these are precisely the two elements which are 1 mod 3 and ± 1 mod 5.