16

Power permutations on prime residue classes

Fischer Harald[*] *and Stingl Christian*
University of Klagenfurt
Institute of Mathematics, University of Klagenfurt, Universitätsstraße 65 - 67, 9020-Klagenfurt, Austria. Telephone: ++43 463 2700 433. Fax: ++43 463 2700 427. email: harald.fischer@uni-klu.ac.at *and* christian.stingl@uni-klu.ac.at

Abstract

Nöbauer proofed in (Nöbauer, 1954) that the power function $x \mapsto x^k \ mod \ n$ is a permutation on Z_n for a positive integer n iff n is squarefree and $(k, \lambda(n)) = 1$, where $\lambda(n)$ denotes the Carmichael function and (a,b) the greatest common divisor of a and b. The RSA-cryptosystem uses this property for $n = pq$, where p, q are distinct primes. Hence the modul cannot be chosen arbitrarily. If we consider permutations on prime residue classes, there is no restriction for the module anymore. In order to find criteria for power permutations on Z_n^* we first deal with the fixed point problem. As a consequence we get the condition for k :

$$(k, [\phi(p_1^{\alpha_1}, \dots, p_r^{\alpha_r}]) = 1 \quad \text{for} \quad n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

where ϕ denotes the Euler totient function and $[a,b]$ the least common multiple of a and b.

Keywords

Power permutations, RSA-cryptosystems, fixed points

1 INTRODUCTION

In (Müller and Nöbauer, 1983) a formula for fixed points of power permutations on Z_n is proofed. If $n = p_1 \cdot \ldots \cdot p_r$ is product of mutually distinct primes p_i and $v = [p_1 - 1, \dots, p_r - 1]$ with $(k, v) = 1$ then the number of fixed points $fix(k, n)$ of the power permutations on Z_n is

[*]This paper was supported by the Österreichischen Fonds zur Förderung der wissenschaftlichen Forschung under FFWF-Project Nr. P09272

R. Posch (ed.), *Communications and Multimedia Security*

Table 1

	Arguments								$\#fix$	with (1)
x	0	1	2	3	4	5	6	7		
x^k *mod* n	0	1	0	3	0	5	0	7	5	3

$$fix(k,n) = \prod_{i=1}^{r}(1 + (k-1, p_i - 1)).$$

Dropping the restricting conditions which are necessary to get permutations gives rise to the question for a universally valid fixed point formula that is independent of the module and the exponent. There is a mistake in several publications, e.g. (Rosen, 1988), that give the universal fixed point formula as follows

$$fix(k,n) = \prod_{i=1}^{r}(1 + (k-1, \phi(p_i^{\alpha_i}))), \tag{1}$$

where $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$. This formula already fails in the simple case, where $n = 2^3$ and $k = 3$ as shown in Table 1.

In order to proof the general case we need some basic definitions and theorems.

Definition 1 *With Z_m^* we denote the set of the units of Z_m. Z_m^* forms an abelian group under multiplication mod m.*

Lemma 1 *If $m = 2^n$ and $n = 1, 2$ then Z_m^* is cyclic.*

Lemma 2 *If $n \geq 3$ and $a \in Z_{2^n}^*$ then $ord_{2^n}(a) | 2^{n-2}$.*

Corollary 1 *If $n \geq 3$ then the group $Z_{2^n}^*$ is not cyclic.*

In general we have

Theorem 1 (Gauss) *Z_m^* is cyclic iff $m = 1, 2, 4, p^e, 2p^e$, where p is an odd prime and e a positive integer.*

Theorem 2 *If $m = 2^n$ and $n \geq 3$ then $ord_m(5) = \phi(m)/2$ and*

$$\{5, 5^2, 5^3, \ldots, 5^{2^{n-2}}, -5, -5^2, -5^3, \ldots, -5^{2^{n-2}}\}$$

is a prime residue system, where $\pm 5^{2^{n-2}} \equiv \pm 1$ mod m.

Lemma 3 *If $(a, m) = 1$, then $a^{\lambda(m)} \equiv 1$ mod m, where m is a positive integer.*

2 THE NUMBER OF FIXED POINTS

Definition 2 *Let $fix(k,n)$ denote the number of fixed points of $x \mapsto x^k$ over Z_n, where k,n are positive integers.*

Lemma 4 *If $p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ is the unique prime factorication of n then*

$$fix(k,n) = \prod_{i=1}^{r} fix(k,p_i^{\alpha_i}).$$

Theorem 3 *Let p an odd prime and α a positive integer then*

$$fix(k,p^\alpha) = \begin{cases} p^\alpha & \textit{for } k=1, \\ 1+(k-1,\phi(p^\alpha)) & \textit{else.} \end{cases}$$

Proof. For $k = 1$ the proposition is obvious. For $k > 1$ we consider the equation

$$x^k \equiv x \ mod\ p^\alpha \iff x(x^{k-1}-1) \equiv 0 \ mod\ p^\alpha. \tag{2}$$

Since for $1 \leq \beta < \alpha : p^\beta | x \Rightarrow p^{\alpha-\beta} \not| \, x^{k-1}-1$ and conversely, (2) is valid iff $x \equiv 0 \ mod\ p^\alpha$ or $x^{k-1} \equiv 1 \ mod\ p^\alpha$. Since $p \neq 2$ there exists as a consequence of theorem 1 a primitiv root ω, hence $\{\omega, \omega^2, \ldots, \omega^{\phi(p^\alpha)}\}$ is a prime residue system. If $x = \omega^t$ then

$$\begin{aligned} x^{k-1} \equiv 1 \ mod\ p^\alpha & \iff \omega^{t(k-1)} \equiv 1 \ mod\ p^\alpha \\ & \iff t(k-1) \equiv 0 \ mod\ \phi(p^\alpha). \end{aligned} \tag{3}$$

But now (3) has exactly $(k-1, \phi(p^\alpha))$ incongruent solutions and therefore

$fix(k,p^\alpha) = 1 + (k-1, \phi(p^\alpha))$. □

In order to get the complete fixed point formula we must consider the case $p = 2$ and $\alpha \geq 1$. We state

Theorem 4 *If $n = 2^\alpha$ and α is a positive integer then the number of fixed points is*

$$fix(k,n) = \begin{cases} 2^\alpha & \textit{for } k=1, \\ 1+(k-1,\phi(2^\alpha)) & \textit{for } \alpha = 1,2 \textit{ or } 2|k, \\ 1+2(k-1,\lambda(2^\alpha)) & \textit{else.} \end{cases}$$

Proof. For $\alpha = 1,2$ and $k = 1$ the proposition is obvious. For $\alpha \geq 3$ and $k \neq 1$ we study the equation

$$x^k \equiv x \ mod\ 2^\alpha \iff x(x^{k-1}-1) \equiv 0 \ mod\ 2^\alpha \tag{4}$$

Analogous to the proof of theorem 3 we conclude, that (4) is valid iff

$$x \equiv 0 \ mod \ 2^\alpha \text{ or } x^{k-1} \equiv 1 \ mod \ 2^\alpha. \tag{5}$$

It is known that $x^{k-1} \equiv 1 \ mod \ 2^\alpha$ which implies $2|x^{k-1} - 1$ and hence $2 \not| \, x$. Therefore $(2^\alpha, x) = 1$ and $x \in Z^*_{2^\alpha}$.
By Lemma 3 and (5) it follows that

$$ord(x)|\lambda(2^\alpha) = 2^{\alpha-2} \quad \text{and} \quad ord(x)|k-1 \tag{6}$$

If $k = 2n$ then only $ord(x) = 1$ satisfies the last condition and and hence $x \equiv 1 \ mod \ 2^\alpha$. From this we get for even k exactly the two fixed points $0, 1$.
If $k = 2n + 1$, where n is a positive integer. From (6) follows that there are only orders of the form 2^ν, where $\nu = 0, 1, \ldots, \alpha - 2$. If $\nu = 0$ then $x \equiv 1 \ mod \ 2^\alpha$ and hence we get only one solution. By using Theorem 2 let $x \in Z^*_{2^\alpha}$ be of the form $x = 5^s$, where $s = 2^t u$ and $t = 0, 1, \ldots, n-3$ and u is odd. Let us consider now the order of x. We get

$$ord(5^s) = \frac{ord(5)}{(s, ord(5))} = \frac{2^{n-2}}{(s, 2^{n-2})} = \frac{2^{n-2}}{2^t} = 2^{n-t-2} = \sigma$$

Since $(-x)^\sigma \equiv 1 \ mod \ 2^\alpha$ hence $ord(-x)|ord(x)$. Similarily we see $ord(x)|ord(-x)$ and so $ord(x) = ord(-x)$. Therefore

$$ord(5^s) = ord(-5^s) = 2^{n-t-2},$$

is independent of u in $s = 2^t u$. Since

$$1 \leq 2^t u \leq 2^{n-2} - 1$$

there are exactly 2^{n-t-3} possibilities to choose u and the same number for -5^s, altogether $2 \cdot 2^{n-t-3} = 2^{n-t-2}$.
The order of $-5^{2^{n-2}} \equiv -1 \ mod \ 2^\alpha$, which we have not considered yet, is 2, and hence there are exactly $2^1 + 1 = 3$ elements of the order $ord(x) = 2$. By (6) the order of x must always divide $k - 1$. If $k - 1 = 2^{\bar{t}} \bar{u}$, where $2 \not| \, \bar{u}$, we just have to derive those elements, whose order divides $2^{\bar{t}}$. These are

$$\begin{aligned} 1 + 3 + \ldots + 2^{\bar{t}} &= 1 + (1 + 2 + \ldots + 2^{\bar{t}}) \\ &= 1 + 2^{\bar{t}+1} - 1 \\ &= 2^{\bar{t}+1} \end{aligned}$$

elements.
If $k-1 \equiv 0$ mod $2^{\alpha-2}$ then $k-1 = 2^{\alpha-2} \cdot l$ and we have

$$x^{k-1} \equiv (x^{2^{\alpha-2}})^l \equiv 1 \ mod \ 2^\alpha.$$

By Lemma 3 this relation holds for all $x \in Z^*_{2^\alpha}$ and these are exactly $\phi(2^\alpha) = 2^{\alpha-1}$ elements.
From the above results we see that the proposition of the theorem is valid. □

3 PERMUTATIONS ON Z^*_N

Definition 3 *Let $L(k,n)$ the number of solutions of the equation $x^k \equiv 1$ mod n, where k,n are positive integers.*

Lemma 5 *The map $f: Z^*_n \to Z^*_n$, with $x \mapsto x^k$ mod n is injectiv iff $L(k,n) = 1$.*

Proof. Since f is a homomorphism, f is injectiv iff $Ker(f) = \{1\}$ and this holds iff $L(k,n) = 1$. □

As a consequence we get the following

Theorem 5 *The map f induces a permutation on Z^*_n iff $L(k,n) = 1$.*

In order to exclude trivial permutations on Z^*_n, where $n = \prod_{i=1}^r p_i^{\alpha_i}$, we have to choose $k \neq 1$, such that

$$\begin{aligned} L(k,n) = 1 \quad &\Longleftrightarrow \quad \prod_{i=1}^{r} L(k, p_i^{\alpha_i}) = 1 \\ &\Longleftrightarrow \quad L(k, p_i^{\alpha_i}) = 1, \quad i = 1, \ldots, r. \end{aligned}$$

Since $L(k,p^\alpha) = fix(k+1, p^\alpha) - 1$ and by Theorem 3, 4 we have

$$L(k,p^\alpha) = (k, (\phi(p^\alpha))$$

for $p \neq 2$ and

$$L(k,p^\alpha) = \begin{cases} (k, \phi(p^\alpha)) & \text{for } \alpha = 1,2 \text{ or } 2 \not| \, k, \\ 2(k, \lambda(p^\alpha)) & \text{for } 2|k. \end{cases}$$

for $p = 2$. Therefore $n = 2^{\alpha_0} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ has to satisfy

$$\left.\begin{array}{r}(k,\phi(2^{\alpha_0}))\\ 2(k,\lambda(2^{\alpha_0}))\end{array}\right\} \cdot \prod_{i=1}^{r}(k,\phi(p_i^{\alpha_i})) = 1.$$

For even k this condition can never hold and hence it can be reduced for odd k to

$$(k,\phi(2^{\alpha_0}))\cdot\prod_{i=1}^{r}(k,\phi(p_i^{\alpha_i})) = 1 \iff (k,[\phi(2^{\alpha_0}),\phi(p_1^{\alpha_1}),\ldots,\phi(p_r^{\alpha_r})]) = 1.$$

Now the demand for the squarefreeness of the p_i in the primfactorization of n can be dropped in the case of Z_n^*.
Analogous to the condition for power permutations on Z_n we state for Z_n^*

Corollary 2 *Let $n = 2^{\alpha_0}\cdot p_1^{\alpha_1}\cdot\ldots\cdot p_r^{\alpha_r}$ and k an odd positive integer. The map f is a permutation on Z_n^* iff $(k,[\phi(2^{\alpha_0}),\phi(p_1^{\alpha_1}),\ldots,\phi(p_r^{\alpha_r})]) = 1$.*

4 THE RSA-CRYPTOSYSTEM ON PRIME RESIDUE CLASSES

The results of the last section motivate a public-key cryptosystem on prime residue classes. Analogous to the classical RSA-cryptosystem the enciphering and deciphering are defined by

$$\begin{array}{lllll} D & : & M & \mapsto & M^d \ mod\ n, \quad M\in Z_n^* \\ E & : & C & \mapsto & C^e \ mod\ n, \end{array}$$

where

$$(d,[\phi(p_1^{\alpha_1}),\ldots,\phi(p_r^{\alpha_r})]) = 1 \quad \text{and} \quad d\cdot e \equiv 1\ mod\ \lambda(n)$$

with $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.
Since $C \equiv M^d\ mod\ n$ we have

$$C^e \equiv M^{d\cdot e} = M^{\lambda(n)\cdot v}\cdot M \equiv M \quad mod\ n$$

To guarantee cryptographical security the prime factors of the parameter n should be strong primes. For more information see (Rivest, Shamir and Adleman, 1978), (Berkovits, 1982), (Gordon, 1984) and (Jamnig, 1984). We can make the system more practicable by choosing the message M from Z_p, where $p := \min_i\{p_i\}$ instead of Z_n^*. This means that each participant publishes the parameters n, d and the length of the blocks $B < p$.

Alternatively there is the possibility to fix the blocklength for the system, e.g. about onehundred digits. This forces each participant to determine each prime factor of n greater than onehundred digits.
Futhermore you should note that the permutation, induced by $x \mapsto x^d \ mod\ n$, has as few fixed points as possible. Because the knowledge of nontrivial fixed points could make it possible to factorize n, see (Williams and Schmid, 1979). Since the number of fixed points is determined by n and d, you can derive this number by

$$fix(d,n) = fix(d,2^{\alpha_0}) \cdot \prod_{i=1}^{r} fix(d,p_i^{\alpha_i}) \geq \begin{cases} 3^r, & \alpha_0 = 0 \\ 2 \cdot 3^r, & \alpha_0 = 1,2 \\ 5 \cdot 3^r, & \alpha_0 \geq 3, \end{cases}$$

where $n = 2^{\alpha_0} \cdot \prod_{i=1}^{r} p_i^{\alpha_i}$.

REFERENCES

Berkovits, S. (1982) Factoring via Superencryption. *Cryptologia*, **6**, 229-37.

Carmichael, R. D. (1910) Note on a Number Theory Function. *Am. Math. Soc.*, **16**, 232-9.

Gordon, J. (1984) Strong Primes are Easy to Find. *Adv. in Cryptology, Proceedings of Eurocrypt 84*, 216-23.

Jamnig, P. (1984) Securing the RSA-cryptosystem against cycling attacks. *Cryptologia*, **12**, 159-64.

Müller, W.B and Nöbauer, W. (1983) Über die Fixpunkte der Potenzpermutationen. *Sitzungsberichte der Österr. Akademie der Wissenschaften, math.-nat. Klasse, Abt. II*, **192**, 93-7.

Nöbauer, W. (1954) Über eine Gruppe der Zahlentheorie. *Monatsh. Math.*, **58**, 181-92.

Nöbauer, W. and Wiesenbauer J. (1981) Zahlentheorie. Prugg - Verlag, Eisenstadt.

Rivest, R.L., Shamir, A. and Adleman, L. (1978) Obtaining Digital Signatures and Public-Key Cryptosystems. *Comm. AMC*, **21**, 120-6.

Rosen, K. H. (1988) Elementary Number Theory and Its Applications. Addison-Wesley, Reading, Mass.

Williams, H.C. and Schmid B. (1979) Some Remarks Concerning the M.I.T. Public-Key Cryptosystem. *Bit*, **19**, 525-38.

BIOGRAPHY

Harald Fischer is a lecturer and Christian Stingl is an assistant at the Institute of Mathematics at the University of Klagenfurt AUSTRIA. Both received their master's degree from University of Klagenfurt in 1994. Since 1994 they have been working on number theory and modern cryptographic methods.