A Note on the Ate Pairing

Chang-An Zhao, Fangguo Zhang and Jiwu Huang

[1] School of Information Science and Technology,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
[2] Guangdong Key Laboratory of Information Security Technology,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
zhcha@mail2.sysu.edu.cn
isszhfg@mail.sysu.edu.cn
isshjw@mail.sysu.edu.cn

Abstract. The Ate pairing has been suggested since it can be computed efficiently on ordinary elliptic curves with small values of the traces of Frobenius t. However, not all pairing-friendly elliptic curves have this property. In this paper, we generalize the Ate pairing and find a series of variations of the Ate pairing. We show that the shortest Miller loop of the variations of the Ate pairing can possibly be as small as $r^{1/\varphi(k)}$ on more pairing-friendly curves generated by the method of complex multiplications, and hence speed up the pairing computation significantly.

Keywords: Tate pairing, Ate pairing, Elliptic curves, Pairing-based cryptosystems.

1 Introduction

Pairing-based cryptosystems have been one of the most active areas in elliptic curve cryptography since 2000. Some detailed summaries on this subject can be found in [20] and [15]. There are three early developing contributions which inspire many other pairing-based cryptographic applications in this area: Sakai *et al.*'s pairing-based key agreement [21], Joux's three-party key agreement [14] and Boneh and Franklin's identity-based encryption scheme [4]. A bottleneck for implementing pairing-based cryptosystems is to compute the pairings.

The pairings can be evaluated in polynomial time by Miller's algorithm [18]. Many useful techniques have been suggested for optimizing the computation of the pairings. Some excellent summaries about pairing computations are recommended (see [12, 22]). One of the most elegant techniques for computing the pairings efficiently is to shorten the iteration loop in Miller's algorithm. Inspired by the Duursma-Lee method for some special supersingular curves in [7], Barreto *et al*. introduce the Eta pairing which has a half length of the Miller loop compared to the original Tate pairing on supersingular Abelian varieties. Later, Hess *et al*. suggest the Ate pairing which shortens the length of the Miller loop obviously on ordinary elliptic curves [13]. Matsuda *et al*. optimize the Ate pairing and the twisted Ate pairing and show that both them are always at least as fast as the Tate pairing [17]. The Ate pairing has been one of the fastest pairings till now.

The length of the Miller loop in the Ate pairing depends on the value of the trace of Frobenius t modulo the subgroup order r. For fast pairing computations, $t - 1 \bmod r$ should be made as small as possible. There do exist some special pairing-friendly elliptic curves with t which can be as small as $r^{1/\varphi(k)}$ [6]. Freeman has also discussed how to generate some elliptic curves which are suitable for the Ate pairing [9]. However, not all pairing-friendly elliptic curves have this excellent property (see examples in [19, 5]), i.e. the Miller loop of the Ate pairing does not achieve $r^{1/\varphi(k)}$ on these pairing-friendly elliptic curves.

In this paper, we tackle this problem by generalizing the Ate pairing. we find a series of the variations of the Ate pairing and explore how to choose the generalized Ate pairing having the Miller loop as small as possible. For more ordinary elliptic curves suitable for pairing-based cryptosystems, the Miller loop of the generalized Ate pairing can reach the lower bound $r^{1/\varphi(k)}$ and hence accelerates pairing computations efficiently.

The rest of this paper is organized as follows. Section 2 introduces basic mathematical concepts of the Tate pairing and the Ate pairing. Section 3 generalizes the Ate pairing and shows how to choose the optimal parameter of the generalized Ate pairing for fast pairing computations. Section 4 gives efficiency considerations. We draw our conclusion and describe further work in Section 5.

2 Mathematical Preliminaries

2.1 Tate Pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where p is a prime. Let E be an elliptic curve defined over $\mathbb{F}_q$ and $\mathcal{O}$ be the point at infinity. $\#E(\mathbb{F}_q)$ is denoted as the order of the rational points group $E(\mathbb{F}_q)$ and r is a large prime satisfying $r|\#E(\mathbb{F}_q)$. Let k be the embedding degree, i.e. the smallest positive integer such that $r|q^k - 1$.

Let $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$. For each integer i and point P, let $f_{i,P}$ be a rational function on E such that

$$(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O}).$$

Let D be a divisor which is equivalent to $(Q) - (\mathcal{O})$ with its support disjoint from $(f_{r,P})$. The Tate pairing [10] is a bilinear map

$$\hat{e} : E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r,$$

$$\hat{e}(P, Q) = f_{r,P}(D).$$

By Theorem 1 in [2], one can define the reduced Tate pairing as

$$e(P, Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}}.$$

The above definition is convenient since a unique element of $\mathbb{F}_{q^k}^*$ is often required in many cryptographic protocols.

2.2 Miller's Algorithm

Let $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$. Let $l_{R,T}$ be the equation of the line through points R and T, and let v_S be the equation of the vertical line through point S. For $i, j \in \mathbb{Z}$, we have

$$f_{i+j,P}(Q) = f_{i,P}(Q) f_{j,P}(Q) \frac{l_{iP,jP}(Q)}{v_{(i+j)P}(Q)}.$$

Using the above formula, $f_{r,P}(Q)^{\frac{q^k-1}{r}}$ can be computed in polynomial time by Miller's algorithm.

Miller's algorithm
Input: $r = \sum_{i=0}^{n} l_i 2^i$, where $l_i \in \{0,1\}$. $P \in E[r]$ and $Q \in E(F_{q^k})$.
Output: $e(P,Q)$
1. $T \leftarrow P$, $f_1 \leftarrow 1$
2. for $i = n-1, n-2, ..., 1, 0$ do
2.1 $f_1 \leftarrow f_1^2 \cdot \frac{l_{T,T}(Q)}{v_{2T}(Q)}$, $T \leftarrow 2T$
2.2 if $l_i = 1$ then
2.3 $f_1 \leftarrow f_1 \cdot \frac{l_{T,P}(Q)}{v_{T+P}(Q)}$, $T \leftarrow T+P$
3. return $f_1^{(q^k-1)/r}$

2.3 Ate Pairing

We recall the definition of the Ate pairing from [13] in this subsection. Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where p is a prime. Let E be an ordinary elliptic curve over $\mathbb{F}_q$, r a large prime with $r \mid \#E(\mathbb{F}_q)$ and let t denote the trace of Frobenius, i.e. $\#E(\mathbb{F}_q) = q + 1 - t$. Let π_q be the Frobenius endomorphism, $\pi_q : E \to E : (x, y) \mapsto (x^q, y^q)$. For $T = t-1$, $Q \in \mathbb{G}_2 = E[r] \cap Ker(\pi_q - [q])$ and $P \in \mathbb{G}_1 = E[r] \cap Ker(\pi_q - [1])$, we have the following:

- $f_{T,Q}(P)$ defines a bilinear pairing, which is called the *Ate* Pairing.
- let $N = gcd(T^k - 1, q^k - 1)$ and $T^k - 1 = LN$, with k the embedding degree, then
$$e(Q,P)^L = f_{T,Q}(P)^{c(q^k-1)/N}$$
where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \mod r$.
- for $r \nmid L$, the *Ate* pairing is non-degenerate.

3 Generalizations of the Ate Pairing

3.1 Generalized Ate pairing

The main result of this paper is summarized in the following theorem.

Theorem 1. *Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where p is a prime. Let E be an ordinary elliptic curve over $\mathbb{F}_q$, r be a large prime with $r \mid \#E(\mathbb{F}_q)$ and let t denote the trace of Frobenius, i.e. $\#E(\mathbb{F}_q) = q + 1 - t$. Let k be its embedding degree and $T = t-1$. For $T^i = (t-1)^i \equiv q^i \mod r$ where $1 \le i \le k-1$,* *we denote $T_i = T^i$ mod r. For $Q \in \mathbb{G}_2 = E[r] \cap Ker(\pi_q - [q])$ and $P \in \mathbb{G}_1 = E[r] \cap Ker(\pi_q - [1])$, we have the following:*

- *$f_{T_i,Q}(P)$ defines a bilinear pairing, which is called the Ate_i Pairing.*
- *let a be the smallest positive integer such that $T_i^a \equiv 1$ mod r. Let $N = gcd(T_i^a - 1, q^k - 1)$ and $T_i^a - 1 = LN$, then*

$$e(Q,P)^L = f_{T_i,Q}(P)^{c(q^k-1)/N}$$

  where $c \equiv \sum_{j=0}^{a-1} T_i^{a-1-j}(q^i)^j$ mod N.
- *for $r \nmid L$, the Ate_i pairing is non-degenerate.*

It is easily checked that such a in Theorem 1 must exist and divide k by Lagrange's Theorem. The proof of Theorem 1 totally parallels the main proof in [13, 17].

Proof of Theorem 1: Note that $r \mid N$ since $T_i^a \equiv 1 \bmod r$ and $q^k \equiv 1 \bmod r$. Thus we have

$$e(Q,P) = f_{r,Q}(P)^{(q^k-1)/r} = f_{N,Q}(P)^{(q^k-1)/N}.$$

Lemma 1 in [13] implies

$$\begin{aligned} e(Q,P)^L =& f_{N,Q}(P)^{L(q^k-1)/N} = f_{LN,Q}(P)^{(q^k-1)/N} \\ =& f_{T_i^a-1,Q}(P)^{(q^k-1)/N} \\ =& f_{T_i^a,Q}(P)^{(q^k-1)/N}. \end{aligned} \tag{1}$$

Using Lemma 2 in [1] and [13], we have

$$f_{T_i^a,Q} = f_{T_i,Q}^{T_i^{a-1}} f_{T_i,T_iQ}^{T_i^{a-2}} \cdots f_{T_i,T_i^{a-1}Q}. \tag{2}$$

Since $\pi_{q^i}^j$ is purely inseparable of degree q^{ij} where $1 \le j < a$ and $\pi_{q^i}^j(Q) = [q^{ij}]Q = [T^{ij}]Q = [T_i^j]Q$ (see [23] pages 29-34), we have

$$\begin{aligned} (\pi_{q^i}^j)^*(f_{T_i,\pi_{q^i}^j(Q)}) =& q^{ij} T_i(Q) - q^{ij}(\pi_{q^i}(Q)) - q^{ij}(T_i - 1)(\mathcal{O}) \\ =& (f_{T_i,Q}^{q^{ij}}). \end{aligned}$$

Note that $(\pi_{q^i}^j)^*(f_{T_i,\pi_{q^i}^j(Q)}) = (f_{T_i,\pi_{q^i}^j(Q)} \circ \pi_{q^i}^j)$ and $f_{T_i,Q}^{q^{ij}} = f_{T_i,Q}^{\sigma^{ij}} \circ \pi_{q^i}^j$ with σ the q-th power Frobenius automorphism of $\overline{\mathbb{F}}_q$, hence we can obtain

$$f_{T_i,\pi_{q^i}^j(Q)} = f_{T_i,Q}^{\sigma^{ij}}.$$

Since $P \in E[r] \cap Ker(\pi_q - [1])$, we have

$$f_{T_i,T_i^j Q}(P) = f_{T_i,\pi_{q^i}^j(Q)}(P) = f_{T_i,Q}^{\sigma^{ij}}(P) = (f_{T_i,Q}(P))^{q^{ij}}. \tag{3}$$

Using the above equality (2), we get

$$f_{T_i^a,Q}(P) = f_{T_i,Q}(P)^{\sum_{j=0}^{a-1} T_i^{a-1-j}(q^i)^j}. \tag{4}$$

Finally, substituting (4) into (1) yields

$$e(Q,P)^L = f_{T_i,Q}(P)^{c(q^k-1)/N}$$

where $c \equiv \sum_{j=0}^{a-1} T_i^{a-1-j}(q^i)^j \bmod N$. This shows that $f_{T_i,Q}(P)$ is a bilinear pairing, which is non-degenerate provided that $r \nmid L$. ■

Theorem 1 shows that a series of the Ate$_i$ pairings $f_{T_i,Q}(P)$ can be obtained as i varies. The reduced Ate$_i$ pairing can be defined as $f_{T_i,Q}(P)^{(q^k-1)/r}$ equal to a fixed power of the reduced Tate pairing. Notice that $T_i = T^i \equiv q^i \bmod r$ and the Miller loop of $f_{T_i,Q}(P)$ is determined by the bit length of T_i. Lastly, it is remarked that the twisted Ate pairing could be generalized easily using the similar idea.

3.2 Selection of the Optimal T_i

In this subsection, we discuss how to choose T_i which has the shortest bit length for fast pairing computations.

By non-degeneracy, T_i can not be ± 1. Note that $T_i = -1$ yields a trivial pairing since $L = 0$ in this case. Let $\phi_d(x)$ be d-th cyclotomic polynomial with its degree $\varphi(d)$ for some positive integer d [16]. Since $x^k - 1 = \prod_{d|k} \phi_d(x)$ and $T_i^k - 1 \equiv 0 \bmod r$, T_i must satisfy the equation $\phi_d(x) \equiv 0 \bmod r$ for some d. For optimal parameters, we should make $d = k$, i.e. the optimal T_i should be a root of $\phi_k(x) \equiv 0 \bmod r$. Hence we can compute $T_i = T^i \equiv q^i \bmod r$ with $(i,k) = 1$, and choose T_i which has the shortest bit length for efficient pairing computations.

An interesting observation is that the optimal T_i is of size $r^{1/\varphi(k)}$ on some pairing-friendly elliptic curves ([6, 19, 5]) although parts of them have large values of Frobenius traces t.

It should be also noted that the optimal T_i maybe not reach the lower bound $r^{1/\varphi(k)}$ in some special cases (see examples in [3]). An open problem is what relations about q, k and r of elliptic curves enable the smallest $q^i \bmod r$ to reach the lower bound $r^{1/\varphi(k)}$.

4 Efficiency Consideration

Hess *et al*. have given an explicit efficiency analysis for computing the original Ate pairing on special pairing-friendly elliptic curves with t as small as $r^{1/\varphi(k)}$ in [13]. Furthermore, the Miller loop of the optimized Ate pairing equals to $T \equiv q \bmod r$ in [17]. This shows that the Ate pairing is at least as efficient as the Tate pairing.

$T \bmod r$ is often of size $\sqrt{q}$, which does not achieve the lower bound $r^{1/\varphi(k)}$ for some pairing-friendly elliptic curves ([19, 5]). However, the optimal T_i can be as small as $r^{1/\varphi(k)}$ on them in the Ate_i pairing. Therefore, the optimal Ate_i pairing can be computed more efficient than the original Ate pairing in [13] or the optimized Ate pairing in [17] in this case. In a sense, the optimal Ate_i pairing seems to be computed efficiently on more pairing-friendly elliptic curves compared to the original Ate pairing.

Some pairing-friendly elliptic curves which have large values of the trace of Frobenius are listed in Appendix. Here we only compare the bit length of the Miller loop for various pairings since these ordinary curves are suitable for different security levels and the cost of finite fields arithmetic depends on various efficient techniques. Notice that the Ate_i pairing in Table 1 has the minimal loop T_i as small as the lower bound $r^{1/\varphi(k)}$. The embedding degrees k for various elliptic curves are also listed in the parenthesis.

Table 1. The comparisons of bit lengths of loops for the pairings

Type	$E_1(10)$	$E_2(11)$	$E_3(22)$	$E_4(28)$	$E_5(18)$	$E_6(26)$	$E_7(34)$
Tate	187	169	237	234	160	160	183
Ate	140	34	191	60	133	93	103
Ate_i	47	17	24	20	27	14	12

5 Conclusions and Further Work

A series of the generalized Ate pairings called the Ate_i pairings $f_{T_i,Q}(P)$ are presented in this paper. We have discussed how to choose the optimal T_i for efficient pairing computations and shown that the Miller loop of the optimal Ate_i pairing can achieve the lower bound $r^{1/\varphi(k)}$ on more pairing-friendly elliptic curves. An open problem is proposed that what relations about q, k and r on pairing-friendly elliptic curves enable the optimal T_i to reach the lower bound $r^{1/\varphi(k)}$.

Acknowledgement

We would like to thank Florian Hess, Mike Scott and Steven Galbraith for their helpful comments and suggestions on an early draft of this manuscript. We also wish to thank the anonymous referees for their useful comments on this manuscript.

References

1. P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott. Efficient pairing computation on supersingular Abelian varieties. *Designs, Codes and Cryptography*, volume 42, number 3. Springer Netherlands, 2007.
2. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. *Advances in Cryptology-Crypto'2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 354-368. Springer-Verlag, 2002.
3. P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. *Proceedings of SAC 2005-Workshop on Selected Areas in Cryptography*, volume 3897 of Lecture Notes in Computer Science, pages 319-331. Springer, 2006.
4. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3): 586-615, 2003.
5. A. Comuta, M. Kawazoe, and T. Takahashi. Pairing-friendly elliptic curves with small security loss by Cheon's algorithm. Preprint, to appear in the 10th International Conference on Information Security and Cryptology, 2007. Also available from http://eprint.iacr.org/2006/427.
6. P. Duan, S. Cui and C.W. Chan. Special polynomial families for generating more suitable elliptic curves for pairing-based cryptosystems. The 5th WSEAS International Conference on Electronics, Hardware, Wireless & Optimal Communications, 2006. Also available from http://eprint.iacr.org/2005/342.

7. I. Duursma, H.-S. Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, *Advances in Cryptology-Asiacrypt'2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 111-123. Springer-Verlag, 2003.
8. D. Freeman. Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10, *Algorithmic Number Theory Symposium ANTS-VII*, volume 4076 of Lecture Notes in Computer Science, pages 452-465. Springer-Verlag, 2006.
9. D. Freeman, M. Scott, E. Teske. A taxonomy of pairing-friendly elliptic curves. Preprint, 2006. Available from http://eprint.iacr.org/2006/372.
10. G. Frey and H-G. Rück. A remark concerning m-divisibility and the discrete logartihm in the divisor class group of curves. *Math. Comp.,* 62(206):865-874, 1994.
11. S. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing, *Algorithm Number Theory Symposium ANTS V*, volume 2369 of *Lecture Notes in Computer Science*, pages 324-337. Springer-Verlag, 2002.
12. S.D. Galbraith. *Pairings - Advances in Elliptic Curve Cryptography.* Cambridge University Press, 2005.
13. F. Hess, N.P. Smart and F. Vercauteren. The Eta pairing revisited. *IEEE Transactions on Information Theory*, vol 52, pages 4595-4602, Oct. 2006.
14. A. Joux. A one round protocol for tripartite DiffieCHellman. *ANTS-4: Algorithmic Number Theory. Springer-Verlag*, volume 1838 of *Lecture Notes in Computer Science*, pages 385-394. Springer-Verlag, 2000.
15. A. Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. *ANTS-5: Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Computer Science*, pages 20-32. Springer- Verlag, 2002.
16. R. Lidl and H. Niederreiter. *Finite Fields.* Number 20 in Encyclopedia of Mathematics and its Applications, 2nd ed., Cambridge University Press, Cambridge, UK, 1997.
17. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings. Preprint, to appear in the 11th IMA International Conference on Cryptography and Coding, 2007. Also available from http://eprint.iacr.org/2007/013.
18. V.S. Miller. Short programs for functions on curves. Unpublished manuscript, 1986.
19. A. Murphy and N. Fitzpatrick. Elliptic curves for pairing applications. Preprint, 2005. Available from http://eprint.iacr.org/2005/302.
20. K.G. Paterson. *Cryptography from Pairing - Advances in Elliptic Curve Cryptography.* Cambridge University Press, 2005.
21. R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. *2000 Symposium on Cryptography and Information Security-SCIS 2000*, pages 26-28, Okinawa, Japan, Jan.2000.

22. M. Scott. Implementing cryptographic pairings. The 10th Workshop on Elliptic Curve Cryptography, 2006.
23. J.H. Silverman, *The arithmetic of elliptic curves*. Number 106 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.

A Pairing-friendly elliptic curves suitable for the $\boldsymbol{Ate_i}$ pairing

Some pairing-friendly elliptic curves with large values of Frobenius traces are cited as follows. $T \equiv q \bmod r$ and the optimal value of T_i are listed.

E_1 with $k = 10$ in [19]

r=1184972659906501436389408869130632556884221748131065689 61(187bits)
q=269165611404982298837667591457479542280678545574962718143 29796
27630878236096516081595057133066956 9 (324 bits)
T=$q \equiv -11357460830624555479475110389492668198 09535 \bmod r$(140 bits)
The optimal $T_i = T^9 \equiv 104334294221056 \bmod r$ (i=9)(47 bits)

E_2 with $k = 11$ in [19]

r=4490443749660797768110189388620003990660796976804 11 (169 bits)
q=13574419192223522033820740163944747702901942978 62
9811734307414911987295931664659240900472 11 (300 bits)
$T = q \equiv 13503834436 \bmod r$(34 bits)
The optimal $T_i = T^6 \equiv 116206 \bmod r$ (i=6)(17 bits)

E_3 with $k = 22$ in [19]

r=146072480042839735410839194855815902380834280400918514359230
300179430401 (237 bits)
q=4538271507199607685224430704260662154879617975700809361897 6
734645298549353613552077513158958602545660520238745221082 53
2592382511(425 bits)
$T = q \equiv$ -85438723049675798409330967691797302008972819367672256 9
216 mod r(191 bits)
The optimal $T_i = T^7 \equiv 13075456 \bmod r$ (i=7)(24 bits)

E_4 with $k = 28$ in [19]

r=20827659027425489963756462886247268966068900480293595663855491908821297 (234 bits)
q=118143400917763386229164321169531765478830849813868372220241582503104530249717254933438182948872577386372276967001960963118937209(426 bits)
$T = q \equiv$ -379891970942617223 mod r(60 bits)
The optimal $T_i = T^5 \equiv$ 724247 mod r(i=5) (20 bits)

E_5 with $k = 18$ in [5]

r=730767328960794658374478759845478477419642392323 (160 bits)
q=14821945697041765687773625382217321241579116867133148076094462814012058758352127 (264 bits)
$T = q \equiv$ 7699855983294175985742107952727180889343 mod r (133 bits)
The optimal $T_i = T^{11} \equiv$ 94906623 mod r (i=11) (27 bits)

E_6 with $k = 26$ in [5]

r=764696222581341148650511408773719240195697919573 (160 bits)
q=18285492543987287680645893866289922483693928837435505359 (184 bits)
$T = q \equiv$ 8551870640210380614813972059 mod r (93 bits)
The optimal $T_i = T^{15} \equiv$ 9779 mod r (i=15) (14 bits)

E_7 with $k = 34$ in [5]

r=10267261474026538061953029801463094309944057146657157201 (183 bits)
q=19326928722523970823211392049806096197843339094443289507368327 (204 bits)
$T = q \equiv$ 8790878313605026490203306721143 mod r (103 bits)
The optimal $T_i = T^{19} \equiv$ 2743 mod r (i=19) (12 bits)