Int. J. Communications, Network and System Sciences, **2011, 4, 675-682**
doi:10.4236/ijcns.2011.411083 Published Online November 2011 (http://www.SciRP.org/journal/ijcns)

Algorithms for Integer Factorization Based on Counting Solutions of Various Modular Equations

Boris S. Verkhovsky
Computer Science Department, New Jersey Institute of Technology, Newark, USA
E-mail: *verb73@gmail.com*
Received September 20, 2011; *revised October* 27, 2011; *accepted November* 6, 2011

Abstract

This paper is a logical continuation of my recently-published paper. Security of modern communication based on RSA cryptographic protocols and their analogues is as crypto-immune as integer factorization (*iFac*) is difficult. In this paper are considered enhanced algorithms for the *iFac* that are faster than the algorithm proposed in the previous paper. Among these enhanced algorithms is the one that is based on the ability to count the number of integer solutions on quadratic and bi-quadratic modular equations. Therefore, the *iFac* complexity is at most as difficult as the problem of counting. Properties of various modular equations are provided and confirmed in numerous computer experiments. These properties are instrumental in the proposed factorization algorithms, which are numerically illustrated in several examples.

Keywords: RSA Cryptography, Integer Factorization, Modular Quadratic Equations, Modular Bi-Quadratic Equation, Equivalent Problems, Rabin Protocol

1. Introduction and Problem Statement

Security of modern communication based on RSA or Rabin cryptographic protocols and their analogues is as crypto-immune as difficult is the integer factorization (*iFac*) [1-3]. This paper is a continuation of the paper [4]. In that paper is considered a factorization algorithm of semi-prime $n=pq$ for two cases: where either both factors p and q are non-Blum primes *i.e.*,

$$p=q=1(\mathrm{mod}4), \tag{1.1}$$

or at least one factor is a non-Blum prime. In this paper an *iFac* algorithm is provided, which also works if both factors p and q are Blum primes, *i.e.*,

$$p=q=3(\mathrm{mod}4). \tag{1.2}$$

The SQUAR-algorithm discussed in [4] is based on several properties (formulated as propositions and conjectures) of dual modular elliptic curves, where b is a positive integer:

$$y^2 = x\left(x^2+b^2\right)\left(\mathrm{mod}\, n\right); \tag{1.3}$$

and

$$y^2 = x\left(x^2-b^2\right)\left(\mathrm{mod}\, n\right). \tag{1.4}$$

Let us reiterate some of these properties and then consider their generalizations.

Let $p=q=1(\mathrm{mod}4)$; $n=pq$; let $P(n,b)$ and $M(n,b)$ denote the number of points on elliptic curves (EC) (1.3) and (1.4) respectively.

For the sake of brevity, we call $P(n,b)$ and $M(n,b)$ the *counts*.

Conjecture 1.1: Consider $n=pq$, and let primes p and q satisfy (1.1);

if
$$P\left(n,1\right) \neq M\left(n,1\right); \tag{1.5}$$

then for every integer b

$$P\left(n,b\right) \neq M\left(n,b\right); \tag{1.6}$$

otherwise, for every integer b

$$P\left(n,b\right) = M\left(n,b\right). \tag{1.7}$$

If n is a prime and (1.5) holds, then for every b also holds

$$\left[P\left(n,b\right)+M\left(n,b\right)\right]/2 = n. \tag{1.8}$$

Remark 1.1: Conjecture1.1 plays an important role in the design of the *iFac* described in [4]; further details are provided in the Appendix.

Proposition 1.2: If the factors p and q are congruent to 1 modulo $n=pq$, then the following identities hold for non-negative integers *m and s*:

if

$$|m-s| \bmod 4 = 2\,; \tag{1.9}$$

then

$$P\left(n, 2^m\right) = M\left(n, 2^s\right). \tag{1.10}$$

Proposition 1.3: If the factors p and q are congruent to 1 modulo $n=pq$, $b_1 \neq b_2$, and

$$P\left(n, b_1\right) = M\left(n, b_2\right),$$

then

$$M\left(n, b_1\right) = P\left(n, b_2\right). \tag{1.11}$$

The proposed *iFac*2 algorithm described below is less restrictive than the integer factorization SQUAR-algorithm described and analyzed in [4], because it is also applicable if both p and q satisfy (1.1).

Proposition 1.4: {modular reduction-in-exponent}: Consider elliptic curves

$$y^2 = x\left(x^2 + b^e\right) (\bmod n)\,; \tag{1.12}$$

and

$$y^2 = x\left(x^2 - b^e\right) (\bmod n)\,; \tag{1.13}$$

where $e \geq 4$; then for every integer $b>0$ and $e>0$ the following identities hold:

$$P\left(n, b^e\right) = P\left(n, b^{e \bmod 4}\right); \tag{1.14}$$

$$M\left(n, b^e\right) = M\left(n, b^{e \bmod 4}\right). \tag{1.15}$$

Proof {by mathematical induction}: Consider substitutions

$$y := Yb^3 \bmod n \text{ and } x := Xb^2 \bmod n\,; \tag{1.16}$$

into (1.12). Then after cancellation of the same term b^6 in both parts of (1.12) we derive the EC

$$Y^2 = X\left(X^2 + b^{e-4}\right) (\bmod n). \tag{1.17}$$

Repeating the substitutions (1.16) and cancellations of term b^6, we derive the proof of (1.14). Analogously we proceed with the proof of (1.15).

A generalized reduction-in-exponent can be formulated for a hyperelliptic curve {HEC}.

Proposition 1.5: Consider HECs

$$y^r = \left(x^d \pm x^t b^e\right) (\bmod n)\,; \tag{1.18}$$

and $Y^r = \left(X^d \pm X^t b^{e \bmod [(d-t)r/m]}\right) (\bmod n)$. (1.19)

If $t<d$ and $\gcd(d, r)=m$, then for every integer $b>0$ both HECs have equal number of points.

Proof: after appropriate substitutions, the proof is analogous to the proof of Proposition 1.4 (details of the proof and an example are provided in the Appendix}.

Special case: if $m=1$ and $t=0$, then

$$Y^r = \left(X^d \pm b^{e \bmod dr}\right) (\bmod n). \tag{1.20}$$

2. *iFac*1 Algorithm Based on EC

SQUAR-algorithm described in paper [4] requires consideration of a sequence of elliptic curves with control parameter b. Namely, for every $b=1,2,3,5,\cdots$ to count the number of points on each EC until *four* distinct counts are found; {see *Example* 2.1 below}.

In the following algorithm we need *at most three* distinct counts. Let $P_i := P\left(n, b_i\right)$.

***The iFac*1 *algorithm*:**

1) Compute $P_1, P_2, \cdots, P_i \neq P_1$ until two distinct integers are found;

2) **if** $sign\left(P_1 - n\right) = sign\left(P_i - n\right)$ (2.1)

then $p := \gcd\left(P_1 + P_i, n\right)$; $q=n/p$; (2.2)

else compute $w := \gcd\left(P_1 + P_i, n\right)$; (2.3)

3) **if** $w>1$, **then** $p:=w$; (2.4)

else find a 3rd distinct count P_k;

4) $p := \gcd\left(P_1 + P_k, n\right)$; $q=n/p$. (2.5)

***Example* 2.1:** For semi-prime n=6525401, the sets S_1, S_2, S_3 and S_4 are as follows:

$$\begin{aligned} S_1 &= \{b = 1,7,11,17,29,31,41,\cdots; L = 7012681\}; \\ S_2 &= \{b = 2,5,13,23,37,\cdots; S = 6055665\}; \\ S_3 &= \{b = 3,19,\cdots; A = 6514053\}; \\ S_4 &= \{b=\underline{\mathbf{43}},53,\cdots; B=6519205\}. \end{aligned} \tag{2.6}$$

Therefore, the SQUAR-algorithm provided in [4] requires at least *fifteen* basic steps, because 43 is the fourteenth prime (2.5). Yet, since

$$P_1 \neq P_2 \text{; and } P_1 \neq P_3 \neq P_2\,; \tag{2.7}$$

then the 1st $factor := \gcd\left(P_1 + P_3, n\right)$.

Hence, instead of counting points

$$P_1, P_2, P_3, P_5, P_7, \cdots, P_{43} \tag{4},$$

in fifteen elliptic curves, we determine both factors of n after three distinct counts.

3. *iFac*1 Validation

Definition 3.1: A pair of counts $\left\{P_i, P_j\right\}$ is called a *resolventa* if $\gcd\left(P_i + P_j, n\right) > 1$.

If w=1 (2.1), then we need to compute the 3rd distinct value {see *Example* 2.1}. However, if $w>1$, then we compute the 1st factor, say, p, and then $q:=n/p$. The following proposition and examples provide explanations.

Proposition 3.1: If primes p and q are selected randomly, then with probability greater than 2/3 we can determine factors of semi-prime n if we know only two distinct counts P_1 and P_i.

Proof: It is demonstrated in the paper [4] that if $p=q=1(\text{mod}4)$, then there exist two positive integers $c<p$ and $d<q$, and four sets S_1, S_2, S_3 and S_4 such that for every b the number of points on the elliptic curves (1.3) and (1.4) is equal either A or B or L or S, where

$$\begin{aligned} A &:= (p+c)(q-d); \\ B &:= (p-c)(q+d); \end{aligned} \tag{3.1}$$

$$\begin{aligned} L &:= (p+c)(q+d); \\ S &:= (p-c)(q-d); \end{aligned} \tag{3.2}$$

{see *Example*2.1}.

For instance, let's analyze

$$\gcd(L+S,\ n); \tag{3.3}$$

where $L+S=2(n+cd)$ (3.2). (3.4)

Let's find under what conditions p divides $L+S$: suppose that

$$n+cd=ph, \tag{3.5}$$

where h is an integer. Then (3.5) implies

that $$(n+cd)\text{mod}p=ph\text{mod}p=0; \tag{3.6}$$

and $$cd\text{mod}p=0. \tag{3.7}$$

Since $c<p$, therefore, p must divide d.

Hence, if $c < p \le d < q$, and $p|d$, (3.8)

then we can find factors p and q after considerations of only two distinct counts P_1 and P_i. Although this case is possible {see *Example* 3.2}, for large primes p and q it is highly improbable.

Analogously, we proceed with an analysis of $\gcd(A+B, n)$.

Example 3.1: Consider n=9037729;

and EC $y^2 = x^3 + x \pmod n$. (3.9)

If $P_1 = A$=8894593; $P_i = B$=9176905; then compute

$$w:=\gcd(A+B, n)=1.$$

Since w=1, it means that we cannot find the factors of n because the combination $\{A, B\}$ is not a *resolventa* {see **Table 3.1**}. Yet, after we find the third distinct value $P_k = L$=9342205; the factorization is accomplished:

$$p=3361 \text{ and } q=2689.$$

***Example* 3.2:** {Highly improbable case}: Consider n=24853. Let's verify that, if we know any two counts, we can find p and q. There are six cases to consider:

1). $P_1 = A$; $P_i = B$; 2). $P_1 = A$; $P_i = L$;

3). $P_1 = A$; $P_i = S$; 4). $P_1 = B$; $P_i = L$;

5). $P_1 = B$; $P_i = S$; 6). $P_1 = L$; $P_i = S$;

Table 3.1. Sums and greatest common divisors.

Sums X+Y	gcd(*X+Y*,*n*)	Resolventas
$A+B=2(n-cd)$	≥ 1	No
$A+L=2(p+c)\mathbf{q}$	q	*Yes*
$A+S=2\mathbf{p}(q-d)$	p	*Yes*
$B+L=2\mathbf{p}(q+d)$	p	*Yes*
$B+S=2(p-c)\mathbf{q}$	q	*Yes*
$L+S=2(n+cd)$	≥ 1	No

where A=17385; B=31161; L=35685; and S=15181. Then for each of these combinations we find a factor of n. Indeed,

$\gcd(A+B,n)=29$; $\gcd(B+L,n)=857$;

$\gcd(B+S,n)=29$; $\gcd(A+L,n)=29$;

$\gcd(A+S,n)=857$; $\gcd(L+S,n)=29$.

Although such case is possible, it is highly improbable if p and q are randomly selected.

***Example* 3.3:** Consider n=8405801 and EC (3.9). Compute P_1=8387409; $P_2 = P_1$; P_3=8995597; and $w:=\gcd(P_1 + P_3, n)$=2801.

Because $w>1$, therefore

$$p:=w \text{ and } q:=n/p=3001.$$

In general, every combination $\{A, L\}$, or $\{A, S\}$, or $\{B, L\}$ or $\{B, S\}$ has a common factor. Hence, if w=1,

then $$\gcd(P_1 + P_k, n) > 1, \tag{3.10}$$

otherwise $$\gcd(P_1 + P_i, n) > 1. \tag{3.11}$$

Since n is a semi-prime, then in each of these cases we compute a factor of n. For instance, if

$$P_1=A \text{ and } P_i = L,$$

then $$A + L = (p+c)q; \tag{3.12}$$

and $$\gcd[(p+c)q, n] = q. \tag{3.13}$$

For more details see **Table A2**.

Although the *iFac*1 algorithm is computationally simpler than the *SQUAR* algorithm, we can further simplify the *iFac* algorithm via application of other modular equations.

4. Modular Quadratic and Bi-quadratic Equations

In this section are considered properties of quadratic, bi-quadratic modular equations and equations with $m \ge 3$, where the moduli are prime or semi-prime.

Proposition 4.1: Consider a modular quadratic equation (MQE)

$$y^2 = x^2 - b \pmod n; \tag{4.1}$$

let $G(n, b)$ denote the number of integer pairs (x, y) {called points on quadratic curve (4.1)} that satisfy (4.1); if n is a prime, then for every non-zero b co-prime with n

$$G(n,b) = n-1;$$

if n is a semi-prime and $n=pq$, then for every non-zero b co-prime with n

$$G(pq,b) = (p-1)(q-1). \quad (4.2)$$

Proof is provided in the Appendix.

Conjecture 4.2: Consider a modular equation $V(p, m, b)$:

$$y^2 = x^{2m} - b \pmod p; \quad (4.3)$$

where p is a prime; let $G(p, m, b)$ denote the number of points on (4.3);
if (4.3) is either a quadratic or bi-quadratic equation (*i.e.*, if $m=1$ or $m=2$), and $p$mod4=3, then

$$G(p,m,b) = p-1. \quad (4.4)$$

if $m=1$ and $p$mod4=1, then (4.4) holds.

Table 4.1. Values of G(*p, m, b*).

*p*mod4	*m*=1	*m*=2	$m \geq 3$: if gcd(*m*,*p*–1)=1
*p*mod4=1	$p-1$	$\neq p-1$	$p-1$
*p*mod4=3	$p-1$	$p-1$	$p-1$

Conjecture 4.3: Consider a modular equation $V(n, m, b)$: let $b>0$;

$$y^2 = x^{2m} - b \pmod n; \quad (4.5)$$

and let $G(n, m, b)$ denote the number of points on (4.5); if both factors p and q are primes, and if (4.5) is either a quadratic or bi-quadratic equation (*i.e.*, if $m=1$ or $m=2$), then for every $b>0$

$$G(pq,m,b) = (p-1)(q-1); \quad (4.6)$$

if an odd prime m is co-prime with $(p-1)(q-1)$, then for every b and m each co-prime with $\varphi(n)$

$$G(n,m,b) = (p-1)(q-1) = \varphi(n). \quad (4.7)$$

Here $\varphi(n)$ is called the Euler totient function.

Table 4.2. Values of G(*pq, m, b*).

	m=1	*m*=2	*m*>3; if $\gcd[m,\varphi(n)]=1$
p=*q*(mod4)=1	$\varphi(n)$	$\neq \varphi(n)$	$\varphi(n)$
p=*q*(mod4)=3	$\varphi(n)$	$\varphi(n)$	$\varphi(n)$
*pq*mod4=3	$\varphi(n)$	$\neq \varphi(n)$	$\varphi(n)$

Numerous computer experiments for $m=2, 3, 5, 7$ confirmed Conjecture 4.3 Thirty six examples in **Table 4.3** demonstrate the correctness of the Conjecture 4.3 for $m=1, 2, 3$, and 5. In italics are shown the cases, where $\gcd[m,\varphi(n)]>1$, *i.e.*, where (4.7) does *not* hold.

Table 4.3. Values of *G*(*pq, m, b*); *m*=1,2,3,5.

	m=1	*m*=2	$m \geq 3$; if $\gcd[m,\varphi(n)]=1$
65,85, 377	48,64, 336 ***ok***	*36,28* *324*	***m*=3**:*32*,64, *224* ***m*=5**: 48,64, 336
77,161 209	60,132 180 ***ok***	60,132 180 ***ok***	***m*=3**: *140,308,20* ***m*=5**: *12*,132, *36*
55,95 187	40,72 160 ***ok***	*20,36,* *140*	***m*=3:** 40, *8*, 160 ***m*=5:** *8*, 72, *32*

{see also **Table 6.1** and **6.2** below}.

The *iFac* algorithm described below is based on Proposition 4.1. This algorithm is computationally efficient if there exists an efficient procedure (an oracle) that counts the points on either the MQE ($m=1$) or bi-quadratic equation ($m=2$) (4.5).

Definition 4.1: {equivalence}: Problem A_1 is equivalent to problem A_2 if their time complexities satisfy the inequality $T(A_1) \leq T(A_2)$.

Definition 4.2: {strong equivalence}: Problems A_1 and A_2 are strongly equivalent if their time complexities T_1 and T_2 satisfy $\Theta(T_1) = \Theta(T_2)$.

Tables 6.1 and **6.2** illustrate Conjecture 4.2 and Conjecture 4.3.

5. *iFac*2 Algorithm

Conjecture 4.3 can be applied to design an *iFac*2 algorithm. As it implied from the following discussion, this algorithm is more efficient than the SQUAR-algorithm proposed in [4]. Yet, for the seemingly simple *iFac*2 algorithm we need to know how to efficiently count the number of points $G(n, m, b)$ on modular Equation (4.5) for $m=1$ or $m=2$.

The algorithm

1) Select $b=m=1$; compute $G(n)$ for $V(n,1,1)$ (4.5) and (4.6);

2) Compute

$$R := n - G(n) + 1; \quad (5.1)$$

3) Solve quadratic equation

$$z^2 - Rz + n = 0; \quad (5.2)$$

suppose z_1 and z_2 are its roots;

4) {Integer factors p and q}:

$$p := z_1 \text{ and } q := z_2. \quad (5.3)$$

Therefore, the *iFac*2 problem is equivalent to the problem of counting points on the MQE (4.1).

Remark 5.1: It is well-known that, if n is a semi-prime and if we know the value of Euler totient function $\varphi(n)$ (4.7), then we can find the factors of n. The Conjecture 4.3 is the framework that allows us to compute $\varphi(n)$.

***Example* 5.1:** Let n=98,743,069;
then

$$G(n)=98,723,196;$$

and

$$R := n - G(n) + 1 = 19874.$$

The quadratic equation

$$z^2 - 19874z + 98743069 = 0; \quad (5.4)$$

has two roots:

$$z_{1,2} = 9937 \pm 30.$$

Table 6.1. $V(p, m, 1)$: $y^2 = x^{2m} + 1 (\mathrm{mod} p)$.

p	m = 2	m = 3	m = 5	m = 7	*	p	m = 2	m = 3	m = 5	m = 7
59	58	58	58	58	*	**2011**	2010	*2186*	*2162*	2010
101	*98*	100	*92*	100	*	**2017**	*1998*	*2084*	2016	*2284*
1777	*1854*	*1748*	1776	1776	*	**99923**	99992	99992	99992	99992
1913	*1998*	1912	1912	1912	*	**99991**	99990	*101102*	*101102*	99990

Table 6.2. $V(p, m, 1)$ for $10^6 < p < 10^7$.

p	m = 1	m = 2	m = 3	m = 5	m = 7
2,696,527	2696526	2696526	***2689958***	2696526	***2701694***
5,264,647	5264646	5264646	***5273726***	5264646	5264646
6,878,407	6878406	6878406	***6875918***	6878406	6878406

Hence,

$$p := z_1 = 9967 \text{ and } q := z_2 = 9907.$$

6. Properties of Modular Equations for m>1: Computer Experiments

Table 6.1 describes results of computer experiments for various primes p and

$$y^2 = x^{2m} + 1 (\mathrm{mod}\ p). \quad (6.1)$$

Remark 6.1: In **Tables 6.1** and **6.2** in italic are indicated cases where $G(m, p) \neq p - 1$ if $\gcd(m, p-1) \neq 1$. Notice that since

$$101 \equiv 1777 \equiv 1913 \equiv 2017 \equiv 1 (\mathrm{mod} 4),$$

the bi-quadratic modular equations do not have exactly p–1 points.

7. *iFac*2 Algorithm Validation

From Conjecture 4.3, the number of points $G(n,m)$ on modular Equation (4.5) is equal

$$G(pq, m) = (p-1)(q-1). \quad (7.1)$$

If there is a computationally efficient algorithm that computes $G(n,1)$ or $G(n,2)$, then it implies that for $m \leq 2$

$$p + q = n + 1 - G(n, m). \quad (7.2)$$

Therefore, by the Vieta theorem, p and q are the roots of quadratic equation

$$z^2 - [n + 1 - G(n, m)] z + n = 0. \quad (7.3)$$

Q.E.D

8. Conclusions

Several factorization algorithms were described and analyzed in [4] and in this paper {see **Table 8.1**}. It is obvious that modular Equation (4.5) can be used for the *iFac*2 only if either m=1 or m=2. From the paper it follows that the complexity of integer factorization is at most as difficult as the problem of counting how many solutions have modular Diophantine equations. Therefore, the problem of counting points on the MQE is equivalent with the *iFac*2 problem.

Table 8.1. Algorithms & residues modulo 4.

Algorithm	*Case*1	*Case*2
SQUAR	Four ECs: (8.1)-(8.8); [4]	*Not applicable*
***iFac*1**	Three ECs: (2.1)-(2.6)	*Not applicable*
***iFac*2**	One MQE: (5.1)-(5.4)	One MQE: (5.1)-(5.4)

***Case*1**: p=q=1(mod4) or (p+q)mod4=0;
Case2: p=q=3(mod4).

9. Acknowledgements

I express my appreciation to A. Joux, D. Kanevsky, A. Koval, R. Rubino and to reviewers for suggestions that improved this paper.

10. References

[1] R. L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signature and Public-Key Cryptosystems," *Communications of ACM*, Vol. 21, No. 2, 1978, pp. 120-126. doi:10.1145/359340.359342

[2] H. Elkamchouchi, K. Elshenawy and H. Shaban, "Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers," *Proceedings of the 8th International Conference on Communication Systems*, Singapore City, Vol. 1, 25-28 November 2002, pp. 91-95.

[3] M. O. Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization," *Technical Report MIT/LCS/TR-212*, MIT Laboratory for Computer Science, Cambridge, January 1979.

[4] Boris S. Verkhovsky, "Integer Factorization of Semi-primes Based on Analysis of a Sequence of Modular Elliptic Equations," *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 10, 2011, pp. 609-615. doi:10.4236/ijcns.2011.410073

[5] C. Pomerance, "The Quadratic Sieve Factoring Algorithm," *Advances in Cryptology, Proceedings of Eurocrypt'84, LNCS*, Vol. 209, Springer-Verlag, Berlin, 1985, pp. 169-182.

[6] R. Schoof, "Counting Points on Elliptic Curves over Finite Fields," *Journal de Theorie des Nombres de Bordeaux*, Vol. 7, No. 1, 1995, pp. 219-254. doi:10.5802/jtnb.142

[7] K. Rubin and A. Silverberg, "Ranks of Elliptic Curves," *Bulletin (New Series) of the American Mathematical Society*, Vol. 39, No. 4, 2002, pp. 455-474.

[8] L. Dewaghe, "Remarks on the Schoof-Elkies-Atkin Algorithm," *Mathematics of Computation*, Vol. 67, No. 223, 1998, pp. 1247-1252. doi:10.1090/S0025-5718-98-00962-4

[9] C. F. Gauss, "Theoria Residuorum Biquadraticorum," 2nd Edition, Chelsea Publishing Company, New York, 1965, pp. 534-586.

Appendix

A1. Proof of Proposition 4.1

Consider MQE:

$$y^2 = x^2 - b \pmod n. \quad (A.1)$$

Proposition 4.1: If n is a prime, then the number of points with non-negative x and y on quadratic curve $Q(n)$ is equal n–1; if $n=pq$, then $Q(pq)=(p-1)(q-1)$.

Proof: Consider an integer parameter t on interval $[1, n-1]$. The modular multiplicative inverse of t exists if and only if gcd $(t, n)=1$.

Consider $v = \left(t + t^{-1}b\right)(n+1)/2 \pmod n$;

and

$$w = \left(t^{-1}b - t\right)(n+1)/2 \pmod n. \quad (A.2)$$

If n is a prime, then there are n–1 integers that are co-prime with n; if n is a semi-prime and $n=pq$, then there are $(p-1)(q-1)$ integers that are co-prime with n. If n is odd, then $(n+1)/2$ is an integer; therefore both v and w are integers.

It is easy to verify that for every $\underline{t}$ there is a unique pair $\{v, w\}$ that satisfies (A.1). Therefore, we proved that (A.1) has at least n–1 solutions for n prime and has at least $(p-1)(q-1)$ if $n=pq$. Let us show that there are no other solutions.

Let assume that there ***exists*** a solution (g, h) that is distinct from every pair in (A.2). First of all, $g^2 - h^2 = b \pmod n$, which implies that, if $1 \le b \le n-1$, then neither $(g-h) \bmod n = 0$;

nor

$$(g+h) \bmod n = 0. \quad (A.3)$$

Consider an integer

$$u := (g-h) \bmod n \ne 0; \quad (A.4)$$

where $1 \le u \le n-1$;

then

$$g + h = u^{-1}b \bmod n. \quad (A.5)$$

Thus,

$$g = \left(u + u^{-1}b\right) \times 2^{-1} \bmod n; \quad (A.6)$$

and

$$h = \left(u^{-1}b - u\right) \times 2^{-1} \bmod n. \quad (A.7)$$

If n is *odd*, then modular inverse of 2 exists and

$$2^{-1} \bmod n = (n+1)/2 \bmod n. \quad (A.8)$$

Hence, the solution (g, h) has the same parametric representation as (v, w), if $u=t$. The contradiction proves the Proposition 4.1. Q.E.D.

***Example* A1:** Consider Q(17):

$$y^2 = x^2 - 2 \pmod{17}.$$

There are *sixteen* points on Q(17):

$$(\pm 6, 0); (0, \pm 7); (\pm 1, \pm 4); (\pm 2, \pm 6); (\pm 7, \pm 8).$$

A2. Complexity Analysis

There are several algorithms that count points on elliptic and hyper-elliptic curves. If some of these algorithms can be applied for counting points on quadratic or bi-quadratic modular equations with the same time complexities, then the Schoof-Elkies-Atkin (SEA) algorithm is currently the best known algorithm that counts points on a modular cubic curve with expected running time $O\left(\log^4 p\right)$ [5-7]. Therefore, if, for instance, p is of order $O\left(2^{1024}\right) = O\left(10^{307}\right)$, then

$$O\left(\log^4 p\right) = O\left(2^{40}\right) = O\left(10^{12}\right). \quad (A.5)$$

Because the SEA algorithm does not work if $a=1$ and $b=0$ [8], consider a modular equation $y^2 = x^2 + b^2 \pmod p$ with $|b| \ne 0$ and an algorithm with complexity $O\left(\log^s p\right)$ that counts points on this curve. Since there are algorithms with complexity $O\left(\log^8 p\right)$ that count points for every elliptic curve, therefore $s \le 8$. Thus

$$O\left(\log^s p\right) = O\left(2^{10s}\right) = O\left(10^{3s}\right). \quad (A.6)$$

This implies that in the worst case the problem can be solved with complexity $O\left(10^{24}\right)$.

A3. Proof of Proposition 1.5

Consider hyperelliptic curves (HECs)

$$y^r = \left(x^d + x^t b^e\right) \pmod n; \quad (A.7)$$

and

$$Y^r = \left(X^d + X^t b^{e \bmod [(d-t)r/m]}\right) \pmod n. \quad (A.8)$$

If $0 \le t < d$ and gcd$(d,r)=m$, then for every positive integer b both HECs have equal number of points.

Proof: Consider substitutions

$$x := Xb^w; y := Yb^z; \quad (A.9)$$

into Equation (A.7); then we derive

$$Y^r b^{rz} = \left(X^d b^{dw} \pm X^t b^{tw+e}\right) \pmod n. \quad (A.10)$$

Now let us find such integers w and z, for which the following equation holds

$$rz = dw\left(\mathrm{mod}\varphi(n)\right). \qquad (A.10)$$

The case is simplified if $t \ll \varphi(n)$ and $d \ll \varphi(n)$.

If gcd(r, d)=m; then $w=r/m$ and $z=d/m$.

Hence, $dr \le rt + em$, *i.e.* $(d-t)r/m \le e$.

Therefore, after cancellation of equal terms in both sides of the modular Equation (A.10), we derive a HEC

$$Y^r = \left(X^d \pm X^t b^{e-(d-t)r/m}\right)(\mathrm{mod}\, n). \qquad (A.11)$$

***Example* A3:** Let consider HEC

$$y^6 = \left(x^{15} + x^{11}b^{1777}\right)(\mathrm{mod}1913); \qquad (A.12)$$

then HEC $Y^6 = \left(X^{15} + bX^{11}\right)(\mathrm{mod}1913)$ has the same number of points as (A.12).

Table A1. # of EC and sequence in which *A*, *B*, *L* and *S* are computed; here *S*<*A*<*B*<*L*.

n	P_1; *b*=1	P_2; *b*	P_3; *b*	P_4; *b*	*p*	*q*
3434941	***B***=3537485;1	***L***=3633945;2	*A*=3328341;5	*S*=3239993;-5	1933	1777
4016813	***B***=4034637;1	***S***=3748057;2	*L*=4294809;5	*A*=3989749;-5	2113	1901
4647169	***A***=4552177;1	***B***=4731865;11	***S***=4330189;13	*L*=4974445;17	3121	1489
4915189	***S***=4557869;1	***A***=4836777;2	*B*=4980665;7	*L*=5285445;-7	1489	3301
6295057	***B***=6394801;1	***L***=6509965;5	*S*=6082957;7	*A*=6192505;11	2017	3121
9037729	***A***=8894593;1	***S***=8737213;11	*B*=9176905;13	*L*=9342205;19	3361	2689
9906433	***L***=10181817;1	***S***=9633073;2	***A***=9717861;5	*B*=10092981;7	5021	1973

Remark A1: In five of seven experiments, the very first two counts {*B*, *L*}; {*B*, *S*}; {*S*, *A*}; {*B*, *L*}; and {*A*, *S*} are *resolventas*, *i.e.* they provide a factor of n:

$$p := \gcd\left(P_1 + P_2, n\right).$$

