ACTA ARITHMETICA
XIX (1971)

On the probability that n and $f(n)$ are relatively prime II

by

R. R. Hall (York)

Let $f(n)$ be an additive function and set

$$T(x) = \sum_{\substack{n\leqslant x \\ (n,f(n))=1}} 1.$$

Our ultimate object is to find the weakest conditions on f which ensure that

$$T(x) \sim \frac{6}{\pi^2}x.$$

In the preceding paper [1] we showed that in the particular case

$$f(n) = \sum_{p|n} p, \tag{1}$$

we have

$$T(x) = \frac{6}{\pi^2}x + O\left(\frac{x}{(\log_3 x)^{1/4}(\log_4 x)^{3/4}}\right)$$

where we use the familiar notation $\log_k x$ for iterated logarithms. Our immediate object is to extend this result, and we are able to replace the p in (1) by a class of functions of p which include the polynomials as a special case.

The integer valued function $g(n)$ will be called a *pseudo-polynomial* if

$$g(n+k) \equiv g(n) \bmod k$$

for all n and k. Every polynomial with integer coefficients is a pseudo-polynomial, but not all pseudo-polynomials are polynomials, and I am grateful to Dr. Woodall at Nottingham University for constructing an example, which will be described later. We have

THEOREM 1. *Let $g(n)$ be a pseudo-polynomial. For each prime p define*

$$B(p) = \max_{0\leqslant b\leqslant p-1} \sum_{\substack{a=1 \\ g(a)\equiv b \bmod p}}^{p} 1$$

and suppose that g satisfies the following conditions:

(i) *For each square-free q there exists an a, prime to q, for which*

$$g(a) \not\equiv 0 \bmod q.$$

(ii) *The series*

$$\sum_p \frac{1}{p}\left(\frac{B(p)}{p}\right)^{1/2}$$

is convergent; and

(iii) $$\log(1+|g(n)|) = O(n^{-4/\log_3 n}).$$

Suppose that

$$f(n) = \sum_{p|n} g(p).$$

Then there exists an absolute constant C, independent of g such that

$$T(x) = \sum_{\substack{n<x\\(n,f(n))=1}} 1 = \frac{6}{\pi^2}x + O\left(x \sum_{p \geqslant C\log_3 x} \frac{1}{p}\left(\frac{B(p)}{p}\right)^{1/2} + \frac{x}{\sqrt{\log_3 x}}\right).$$

Two questions naturally present themselves:

(a) Does every polynomial satisfy these conditions?

(b) Is there a pseudo-polynomial, which satisfies the conditions and is not a polynomial?

The answer to (a) is no, even if we restrict ourselves to polynomials whose coefficients have highest common factor 1. For example, $g(n) = n^2+3n+2$ does not satisfy condition (i) for $q = 6$. However, with a slight modification we are more successful:

THEOREM 2. *Let $g^*(n)$ be any polynomial with integer coefficients. Then there exists a constant $m = m(g^*)$ depending on g^*, such that the new polynomial defined by*

$$g(n) = g^*(n) + m(g^*)$$

satisfies the conditions of Theorem 1.

I am unable to provide the answer to question (b). However, it will be shown that the Woodall pseudo-polynomial can be constructed to satisfy the first two conditions.

I am grateful to Professor Erdös for finding the proof of Lemma 2 during his visit to Nottingham in 1969.

Proofs of the Theorems. We give proof of Theorem 2 first, as it is shorter.

Suppose that g^* is of degree d; thus for any choice of m,

$$g(n) = O(n^d)$$

and for every p,

$$B(p) \leqslant d.$$

Thus conditions (ii) and (iii) are satisfied, and in fact are very weak for polynomials.

The number of solutions of

$$g(n) = g^*(n) + m \equiv 0 \bmod q$$

is at most $d^{\nu(q)}$, whatever the choice of m, since q is square-free. Since

$$\nu(q) \ll \frac{\log q}{\log\log q}$$

it follows that for each d there exists a constant $Q = Q(d)$ such that for $q \geqslant Q$,

(2) $$d^{\nu(q)} < \varphi(q)$$

and hence that every polynomial of degree d satisfies condition (i) except perhaps for some values of q less than $Q(d)$.

We can choose $m = m(g^*)$ such that

$$g(1) = g^*(1) + m \not\equiv 0 \bmod p$$

for every prime $p < Q$, by the Chinese remainder theorem. It follows that for $q < Q$, there is at least one a, namely $a = 1$, such that

$$g(a) \not\equiv 0 \bmod q, \quad (a, q) = 1,$$

and for $q \geqslant Q$ the conclusion follows from (2). This completes the proof.

Proof of Theorem 1. We only give those details of the proof which differ materially from the proof contained in [1].

LEMMA 1. *For $p \leqslant \sqrt{x}$ and all a,*

$$\sum_{\substack{m\leqslant x\\ f(m)\equiv a \bmod p}} |\mu(m)| \ll x\left(\frac{B(p)}{p} + \frac{\log p}{\log x}\right).$$

This is proved as in [1]; as before our next step is to replace this estimate over square-free m by a similar one for all m. The following lemma replaces Lemma 3 of the previous paper, the proof being due to Professor Erdös.

In the next paper of this series we prove rather more: for each fixed r we have

$$\sum_{m\leqslant x} Q^r(x, m) \ll x$$

and this enables us to use Hölder's inequality in place of the Cauchy–Schwarz inequality in the application. Therefore the exponent $1/2$ of $B(p)/p$ in Theorem 1 could be improved to any fixed number < 1.

LEMMA 2. *Let $Q(x,m)$ denote the number of integers $n \leqslant x$ whose square-free kernel, that is*

$$\prod_{p|n} p,$$

is equal to m. Then

$$\sum_{m\leqslant x} Q^2(x, m) \ll x.$$

Proof. We have

$$\sum_{m\leqslant x} Q^2(x, m) = \sum_{k=1}^{\infty} k^2 \sum_{\substack{m\leqslant x\\ Q(x,m)=k}} 1 \leqslant \sum_{k=1}^{\infty} k^2 \sum_{\substack{m\leqslant x\\ Q(x,m)\geqslant k}} 1$$

so that it is sufficient to show that for each k the number of m's for which $Q(x, m) \geqslant k$ does not exceed Ax/k^4 for some constant A independent of k and x. For the m's not exceeding x/k^4 we make the simple estimation

$$\sum_{\substack{m\leqslant x/k^4\\ Q(x,m)\geqslant k}} 1 \leqslant x/k^4.$$

Next, let $m > x/k^4$, and suppose m has s distinct prime factors not exceeding k^4. If n has square-free kernel m and $n \leqslant x$,

$$n = mp_1^{a_1}p_2^{a_2}\dots p_s^{a_s}, \qquad a_i \geqslant 0$$

and we are looking for the number of solutions of the inequality

$$a_1\log p_1 + a_2\log p_2 + \dots + a_s\log p_s \leqslant \log\frac{x}{m}, \qquad a_i \geqslant 0;$$

which does not exceed the number of solutions of

$$(a_1 + a_2 + \dots + a_s)\log 2 \leqslant 4\log k.$$

Let $V_r(y)$ be the number of solutions of the inequality

$$\beta_1 + \beta_2 + \dots + \beta_r \leqslant y, \qquad \beta_i \geqslant 0.$$

Plainly

$$V_r(y) = \sum_{\beta_r=0}^{[y]} V_{r-1}(y-\beta_r) \leqslant \int_0^{y+1} V_{r-1}(t)\,dt,$$

V being monotonic, and since $V_1(y) \leqslant y+1$ it follows by induction that

$$V_r(y) \leqslant \frac{(y+r)^r}{r!}.$$

Thus if $m > x/k^4$,

$$Q(x, m) \leqslant \frac{(c\log k + s)^s}{s!}, \qquad c = \frac{4}{\log 2},$$

where s is the number of prime factors of m not exceeding k^4. If $Q(x, m) \geqslant k$, setting $s = u\log k$ and noting that $s! \geqslant (s/e)^s$, we deduce that

$$\left(\frac{c\log k + u\log k}{\frac{u}{e}\log k}\right)^{u\log k} \geqslant k = e^{\log k}$$

and so

$$\left\{e\left(1+\frac{c}{u}\right)\right\}^u \geqslant e.$$

Hence $u \geqslant c'$, an absolute constant which could be derived from the value of c. Hence m must have at least $c'\log k$ distinct prime factors not exceeding k^4, and the number of such m's does not exceed

$$\sum_{p_1\leqslant k^4}\sum_{p_2\leqslant k^4}\dots\sum_{p_s\leqslant k^4}\sum_{\substack{m\leqslant x\\ p_1p_2\dots p_s|m}} 1 \leqslant \frac{x}{s!}\left(\sum_{p\leqslant k^4}\frac{1}{p}\right)^s \leqslant x\left(\frac{e}{s}\sum_{p\leqslant k^4}\frac{1}{p}\right)^s$$

where s is the least integer not less than $c'\log k$. Now there exists an absolute constant c'' such that

$$\sum_{p\leqslant k^4}\frac{1}{p} \leqslant \log\log k + c''$$

and a constant k_0 such that for $k \geqslant k_0$,

$$e(\log\log k + c'') \leqslant \frac{c'\log k}{e^{4/c'}}$$

and for these k the sum above does not exceed x/k^4. For $k \leqslant k_0$ it does not exceed $c'''x \leqslant Bx/k^4$ where c''' and $B = c'''k_0^4$ are again absolute constants. Putting these results together we find that the number of m's for which $Q(x, m) \geqslant k$ does not exceed

$$\frac{x}{k^4} + \max(1, B)\frac{x}{k^4} \leqslant \frac{Ax}{k^4}$$

which completes the proof.

LEMMA 3. *For all $p \leqslant \sqrt{x}$ and all a,*

$$\sum_{\substack{n\leqslant x\\ f(n)\equiv a \bmod p}} 1 \ll x\left(\sqrt{\frac{B(p)}{p}} + \sqrt{\frac{\log p}{\log x}}\right)$$

Proof. Denoting the sum on the left by S we have,

$$S = \sum_{\substack{m\leqslant x\\ f(m)\equiv a \bmod p}} |\mu(m)| Q(x, m)$$

and so by the Cauchy–Schwarz inequality,

$$S^2 \leqslant \Big(\sum_{m\leqslant x} Q^2(x, m)\Big)\Big(\sum_{\substack{m\leqslant x\\ f(m)\equiv a \bmod p}} |\mu(m)|\Big) \ll x^2\left(\frac{B(p)}{p}+\frac{\log p}{\log x}\right)$$

by the last two lemmas. The result follows.

Lemma 4. *Under the conditions on g given in the theorem, for each q we have*

$$\sum_{\substack{n\leqslant x\\ f(nq)\equiv 0 \bmod q}} 1 = \frac{x}{q} + O\left(\frac{x\exp(C_1\sqrt{q}\log q)}{(\log x)^{1/q^3}}\right)$$

where C_1 is an absolute constant, independent of g.

Proof. We follow Lemmas 6 and 7 of [1]. Setting

$$F_q(s, l/q) = \sum_{n=1}^{\infty}\frac{1}{n^s}\exp\{2i\pi(f(nq)-f(q))l/q\},$$

we find that

$$\frac{1}{q}\sum_{l=1}^{q} e^{2i\pi l f(q)/q} F_q(s, l/q) = \sum_{\substack{n=1\\ f(nq)\equiv 0 \bmod q}}^{\infty} n^{-s}.$$

Since $F_q(s, 1) = \zeta(s)$, the result will follow if we can show that for those $l < q$, F is regular and not too large in some region to the left of the line $\boldsymbol{R}s = 1$. Now

$$F_q(s, l/q) = F_q^*(s, l/q)\prod_{\chi}\{L(s, \chi)\}^{\tau_g(\chi, l)/\varphi(q)}$$

where F_q^* is regular and bounded by q^{ε} for $\boldsymbol{R}s > \frac{1}{2}$. It involves the prime factors of q itself. Here

$$\tau_g(\chi, l) = \sum_{a=1}^{q}\bar{\chi}(a)e^{2i\pi g(a)l/q}.$$

The first half of the proof is identical to the old Lemma 7. However, we then used the fact that for $(l, q) = 1$,

$$\sum_{a=1}^{q}\bar{\chi}_0(a)e^{2i\pi al/q} = \mu(q);$$

in fact, all that is required is that its real part is bounded away from $\varphi(q)$, that is, that no F_q has a simple pole at $s = 1$. Now in the present case,

$$1-\boldsymbol{R}\frac{\tau_g(\chi_0, l)}{\varphi(q)} = \frac{1}{\varphi(q)}\sum_{\substack{a=1\\ (a,q)=1}}^{q} 2\sin^2\frac{\pi g(a)l}{q} \geqslant \frac{1}{q^3} \qquad ((l, q) = 1)$$

under the condition of the theorem that $g(a) \not\equiv 0 \bmod q$ for some a prime to q. The rest of the proof follows as before.

Lemma 5. *We have that*

$$\sum_{H\leqslant p\leqslant x}\ \sum_{\substack{m\leqslant x/p\\ f(mp)\equiv 0 \,(\mathrm{mod}\, p)}} 1 = O\left(\frac{x\log_3 x}{\log\log x}\right)$$

provided

$$\log H \geqslant 2A(\log x)/(\log_3 x).$$

Proof. Either $f(mp) = f(m)$ or $f(m)+g(p)$ according to whether $p|m$ or not. Now $g(p) \equiv g(0) \,(\mathrm{mod}\, p)$ so the summation condition is that $p|f(m)$ or $f(m)+g(0)$; if we allow either possibility the sum will be increased. We invert the order of summation and estimate the number of prime factors of $f(m)$ and $f(m)+g(0)$. The above sum does not exceed

$$\sum_{m\leqslant x/H}\ \sum_{\substack{H<p\leqslant x/m\\ p|f(m) \text{ or } f(m)+g(0)}} \leqslant \sum_{\substack{m\leqslant x/H\\ f(m)=0 \text{ or } -g(0)}} \pi\left(\frac{x}{m}\right) + 2\sum_{\substack{m\leqslant x/H\\ f(m)\neq 0 \text{ or } -g(0)}} \frac{\log(|f(m)|+|g(0)|)}{\log H} = S_1 + S_2$$

say. Now

$$f(m) = \sum_{p|m} g(p) = O\left(\frac{\log m}{\log\log m}\max_{n\leqslant m}|g(n)|\right)$$

and so for $f(m) \neq 0$ or $-g(0)$ and $m \leqslant x$,

$$\log(|f(m)|+|g(0)|) = O(x^{A/\log_3 x}).$$

It follows that

$$S_2 \ll \frac{x}{H\log H}x^{A/\log_3 x} = O\left(\frac{x\log_3 x}{\log\log x}\right).$$

We split S_1 into two parts, S_1' and S_1'' according as $f(m) = 0$ or $f(m) = -g(0)$, and it is sufficient to treat S_1' the other case being similar.

For any prime $\tilde{\omega}$ we have

$$S_1' \leqslant \sum_{\substack{m\leqslant x/H\\ f(m)\equiv 0 \,(\mathrm{mod}\,\tilde{\omega})}} \pi\left(\frac{x}{m}\right) \ll \frac{x}{\log H} \sum_{\substack{m\leqslant x\\ f(m)\equiv 0 \,(\mathrm{mod}\,\tilde{\omega})}} \frac{1}{m}.$$

Now

$$\sum_{\substack{m\leqslant x\\ f(m)\equiv 0 \,(\mathrm{mod}\,\tilde{\omega})}} \frac{1}{m} = \int_1^x \Big(\sum_{\substack{m\leqslant y\\ f(m)\equiv 0 \,(\mathrm{mod}\,\tilde{\omega})}} 1 \Big) \frac{dy}{y^2} + \frac{1}{x} \sum_{\substack{m\leqslant x\\ f(m)\equiv 0 \,(\mathrm{mod}\,\tilde{\omega})}} 1$$

$$\ll \int_1^{\tilde{\omega}} \frac{dy}{y} + \int_{\tilde{\omega}}^x \left(\sqrt{\frac{B(\tilde{\omega})}{\tilde{\omega}}} + \sqrt{\frac{\log\tilde{\omega}}{\log y}} \right) \frac{dy}{y} + \sqrt{\frac{B(\tilde{\omega})}{\tilde{\omega}}} + \sqrt{\frac{\log\tilde{\omega}}{\log x}}$$

$$\ll \log\tilde{\omega} + \left(\frac{B(\tilde{\omega})}{\tilde{\omega}}\right)^{1/2} \log x + \sqrt{(\log\tilde{\omega})(\log x)}$$

if $\tilde{\omega} \leqslant \sqrt{x}$. Since the series

$$\sum_p \frac{1}{p}\left(\frac{B(p)}{p}\right)^{1/2}$$

is convergent, its partial sums are bounded and for any K there exists an $\tilde{\omega} \leqslant K$ such that

$$\left(\frac{B(\tilde{\omega})}{\tilde{\omega}}\right)^{1/2} = O\left(\frac{1}{\log\log K}\right).$$

Hence for all $K \leqslant \sqrt{x}$ we have

$$S_1' = O\left(\frac{x}{\log H}\left(\frac{\log x}{\log\log K} + \sqrt{(\log K)(\log x)}\right)\right)$$

and we select

$$\log K = \frac{\log x}{(\log\log x)^2}.$$

Since $\log H \geqslant (2A\log x)/\log_3 x$ we obtain our result.

Proof of the Theorem. Set

$$P(z) = \prod_{p\leqslant z} p.$$

Then for all z,

$$T(x) = \sum_{n\leqslant x} \sum_{\substack{q|P(z)\\ q|(n,f(n))}} \mu(q) + \theta \sum_{p>z} \sum_{\substack{n\leqslant x\\ p|(n,f(n))}} 1$$

where $|\theta| \leqslant 1$.

And therefore

$$T(x) = \sum_{q|P(z)} \mu(q) \sum_{\substack{n\leqslant x/q\\ f(nq)\equiv 0 \bmod q}} 1 + \theta \sum_{p>z} \sum_{\substack{m\leqslant x/p\\ p|f(mp)}} 1$$

$$= x\sum_{q|P(z)} \frac{\mu(q)}{q^2} + \sum_{q|P(z)} \mu(q) \Big\{ \sum_{\substack{n\leqslant x/q\\ f(nq)\equiv 0 \bmod q}} 1 - \frac{x}{q^2} \Big\} +$$

$$+ \theta \sum_{z<p\leqslant H} \sum_{\substack{m\leqslant x/p\\ f(m)\equiv 0 \text{ or } -f(p) \bmod p}} 1 + \theta \sum_{H<p\leqslant x} \sum_{\substack{m\leqslant x/p\\ f(mp)\equiv 0 \bmod p}} 1$$

$$= \frac{6}{\pi^2}x + O\left(\frac{x}{z\log z}\right) + O\left(x\sum_{q|P(z)} \exp\left\{C_1\sqrt{q}\log q - \frac{\log\log x}{q^3}\right\}\right) +$$

$$+ O\left(x\sum_{p>z}\frac{1}{p}\left(\frac{B(p)}{p}\right)^{1/2}\right) + O\left(x\sqrt{\frac{\log H}{\log x}}\right) + O\left(\frac{x\log_3 x}{\log\log x}\right).$$

There exists an absolute constant C_2 such that every

$$q < e^{C_2 z}.$$

Thus for $z = C\log\log\log x$ and $\log H = (2A\log x)/\log_3 x$ we have

$$T(x) = \frac{6}{\pi^2}x + O\left(\frac{x}{\sqrt{\log_3 x}}\right) + O\left(x\sum_{p>C\log_3 x}\frac{1}{p}\left(\frac{B(p)}{p}\right)^{1/2}\right).$$

This completes the proof.

The Woodall pseudo-polynomial. The pseudo-polynomials form a ring, of which the ring $\boldsymbol{Z}[x]$ of polynomials with integer coefficients is a sub-ring. There are several interesting questions we can ask about the algebraic structure of this ring, for example, whether it is an integral domain; all we are going to show now is that there is an infinite class of pseudo-polynomials which are not polynomials.

Choose (integer) values for $g(0)$ and $g(1)$ arbitrarily. We may then select $g(2) \equiv g(0) \bmod 2$ so that it is not the value of the linear function of n determined by $g(0)$ and $g(1)$.

Next, select $g(3) \equiv g(0) \bmod 3$ and $\equiv g(1) \bmod 2$ so that it is not the value of the quadratic function determined by $g(0), g(1)$ and $g(2)$. Proceeding indefinitely, we obtain a pseudo-polynomial which is not a polynomial. Thus $\boldsymbol{Z}[x]$ is a proper sub-ring of the pseudo-polynomials, and a coset of $\boldsymbol{Z}[x]$ (regarded additively or multiplicatively) gives an infinite class; alternatively, each pair of values of $g(0)$ and $g(1)$ gives a different pseudo-polynomial.

Remarks. At each stage of the construction, we have to solve a congruence

$$g(n) \equiv l \bmod N$$

where N is the lowest common multiple of the integers not exceeding n. We may select at least one of the first two solutions of this congruence, so that

$$g(n) \ll e^{An}$$

for some fixed A. But this is not good enough for condition (iii).

Condition (i) is easily arranged by setting $g(1) = 1$.

Condition (ii) is more difficult. Nothing in the construction implies that the numbers $g(0), g(1), g(2), \ldots, g(p-1)$ are well distributed mod p, in fact $B(p)$ could be p. We can make g satisfy (ii) by selecting $g(n)$ to satisfy congruences to moduli $p > n$, but so far as I can see at the expense of dropping condition (iii). Suppose that for $n < p \leqslant t(n)$ (some increasing function of n) we set

$$g(n) \equiv t_p(n) \bmod p$$

where $t_p(n)$ is one of the most deficient residue classes mod p so far. Then for all p,

$$B(p) \leqslant t^{-1}(p)$$

that is, the number of n for which $g(n)$ is not corrected mod p. Roughly we want

$$t^{-1}(p) \leqslant \frac{p}{(\log\log p)^{a}}$$

for some $a > 2$, so that we shall satisfy conditions (i) and (ii) if for example

$$t(n) = n(\log\log n)^{a}.$$

This however, could make $\log(1+|g(n)|)$ too large. The conclusion is that there are infinitely many pseudo-polynomials satisfying the first two conditions, which are not polynomials.

I do not know of any number-theoretic function which presents itself naturally and is a pseudo-polynomial. The chances are that it would satisfy our conditions, and this is one way that the problem could be solved.

Reference

[1] R. R. Hall, *On the probability that n and $f(n)$ are relatively prime*, Acta Arith. 17 (1970), pp. 169–183.

Received on 14. 4. 1970 (81)

ACTA ARITHMETICA
XIX (1971)

О точках конечного порядка эллиптических кривых

В. А. Демьяненко (Свердловск)

Пусть T — кривая первого рода $y^2 = x^4 + ax^2 + b$, определенная над полем рациональных чисел; P — произвольная точка на T; O_m — рациональная точка на T конечного порядка m; $v_q(c) - q$ — показатель числа c; $[t]$ — целая часть числа t; $\{t\}$ — расстояние от t до ближайшего целого числа.

Целью настоящей работы является доказательство следующей теоремы:

Если $m = p^2$, где p — простое > 3, то на кривой $z^p - t^p = 1$, $z^p + t^p = r^p$ $(zt \neq 0)$ лежит не менее $C^2_{(p-1)/2}$ рациональных точек.

Предварительно докажем несколько лемм.

Лемма I. *Координаты точек $kP = \{x_k, y_k\}$ $(k = 1, 2, \ldots)$ можно вычислять по следующим рекуррентным соотношениям:*

$$(1)\quad \begin{cases} x_k = u_k/w_k,\ y_k = v_k/w_k^2,\ u_1 = x_1,\ v_1 = y_1, \quad w_1 = 1; \\ u_k = u_{k/2}^4 - bw_{k/2}^4,\ v_k = v_{k/2}^4 - (a^2-4b)u_{k/2}^4 w_{k/2}^4,\ w_k = 2u_{k/2}v_{k/2}w_{k/2} \\ \qquad\qquad \text{при } k \equiv 0 \pmod 2) \\ \text{и} \\ u_k u_1 = u^2_{\frac{k-1}{2}} u^2_{\frac{k+1}{2}} - bw^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}},\ w_k w_1 = u^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} - u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}}, \\ v_k v_1 = v^2_{\frac{k-1}{2}} v^2_{\frac{k+1}{2}} - (a^2-4b) u^2_{\frac{k-1}{2}} u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} \\ \qquad\qquad \text{при } k \not\equiv 0 \pmod 2). \end{cases}$$

Доказательство. Согласно формулам сложения и вычитания точек на кривой T, имеем:

$$x_k = \frac{x_{k/2}^4 - b}{2x_{k/2}y_{k/2}}, \qquad y_k = \frac{y_{k/2}^4 - (a^2-4b)x_{k/2}^4}{4x_{k/2}^2 y_{k/2}^2}$$