ACTA ARITHMETICA
LXXIII.4 (1995)

The period lengths of inversive congruential recursions

by

Wun-Seng Chou (Taipei)

1. Introduction. Let p be a prime. For fixed elements a and b of the finite field $\mathrm{GF}(p) = \mathbb{Z}/p\mathbb{Z}$ (it can be identified with the set $Z_p = \{0, 1, \ldots, p-1\}$ together with the operations of addition and multiplication modulo p), Eichenauer and Lehn [3] defined sequences $X(x_0; a, b) : x_0, x_1, \ldots$ by choosing initial elements $x_0 \in \mathrm{GF}(p)$ and using the recursion

$$\begin{aligned} &x_{n+1} = a x_n^{-1} + b \quad \text{if } x_n \neq 0, \\ &x_{n+1} = b \quad \text{if } x_n = 0 \end{aligned} \qquad \text{for all } n \geq 0. \tag{1}$$

They used this method as a nonlinear method to generate pseudorandom numbers. Niederreiter [10] generalized it over arbitrary finite field $\mathrm{GF}(q)$ when he studied pseudorandom vectors. See also Eichenauer-Herrmann [5] and Niederreiter [11, Chapters 8 and 10] and [12] for more details on these methods. Because the recursion (1) is used to construct pseudorandom numbers and pseudorandom vectors, the problem of when the sequence $X(x_0; a, b)$ has the maximal period length has been studied intensively: see, for instance, Chou [1], Eichenauer and Lehn [3], Flahive and Niederreiter [8], and Niederreiter [12].

For studying pseudorandom numbers with modulus a composite positive integer m, the recursion (1) must be changed into the following: For all $n \geq 0$,

$$x_{n+1} \equiv a x_n^{-1} + b \bmod m \quad \text{provided} \quad \gcd(x_n, m) = 1. \tag{2}$$

So, every term of $X(x_0; a, b)$ must be relatively prime to m. If $m = p_1^{r_1} \ldots p_t^{r_t}$, where $t \geq 2$ and $p_1, \ldots, p_t$ are distinct primes, is the prime factorization of m, then the period length of $X(x_0; a, b)$ with modulus m equals the least common multiple of period lengths of $X(x_0; a, b)$ with modulus $p_i^{r_i}$, $1 \leq i \leq t$. So, for studying the period length of $X(x_0; a, b)$ with modulus m, it suffices to consider $X(x_0; a, b)$ with modulus a prime power p^k. Eichenauer, Lehn, and Topuzoğlu [4] studied the maximal period length with modulus 2^k. Since the sequence $X(x_0; a, b)$ with modulus a prime divisor p of m instead of m itself does not contain 0 modulo p, $X(x_0; a, b)$ with modulus p does not have the maximal period length. It is necessary to study all possible period lengths of the recursion (1) over $\mathrm{GF}(p)$. Eichenauer and Lehn [3] obtained some results on the period length of $X(x_0;a,b)$ with prime modulus. Chou [2] generalized it over finite fields and got all possible period lengths of the sequence $X(x_0;a,b)$. Also, Eichenauer-Herrmann [6], Eichenauer-Herrmann and Topuzoğlu [7] and Huber [9] studied the period length of $X(x_0;a,b)$ with modulus any prime power.

As we have mentioned above, if the sequence $X(x_0;a,b)$ is generated by the recursion (2), the sequence $X(x_0;a,b)$ with modulus p does not have the maximal period length. To make up for this deficiency, Huber [9] suggested to consider the recursion

$$x_{n+1} \equiv a x_n^{\phi(m)-1} + b \bmod m \quad \text{for all } n \ge 0, \tag{3}$$

where $\phi(m)$ is Euler's totient function. This recursion is equivalent to the recursion (1) when m is a prime number and equivalent to the recursion (2) whenever each term of the sequence $X(x_0;a,b)$ with modulus m is relatively prime to m. But the recursion (3) allows any term x_n of $X(x_0;a,b)$ and m to have a common divisor greater than 1. Huber [9] showed that if m is square free, then $X(x_0;a,b)$ has the maximal period length with modulus m if and only if $X(x_0;a,b)$ with modulus each prime divisor p of m has the period length p.

In this paper, we are going to describe all possible period lengths of sequences $X(x_0;a,b)$ generated by each of recursions (2) and (3). For this purpose, we need the following results from Chou [2].

LEMMA 1. *Let p be a prime and let x_0, a and b be elements of the finite field $\mathrm{GF}(p)$. Let $X(x_0;a,b)$ be the sequence obtained by taking the initial element $x_0 \in \mathrm{GF}(p)$ and using the recursion* (1). *Let $f(x) = x^2 - bx - a$ and let $\mathfrak{o}(m_f)$ be the order of the polynomial $m_f(x) = x^2 + (b^2/a + 2)x + 1$ provided $a \ne 0$. Moreover, let $L(x_0;a,b;p)$ be the period length of $X(x_0;a,b)$.*

(A) *If $a = 0$, then $x_n = b$ for all $n \ge 1$ and so $L(x_0;0,b;p) = 1$.*

(B) *If $a \ne 0$ and $b = 0 = x_0$, then $x_n = 0$ for all $n \ge 0$, and so $L(0;a,0;p) = 1$.*

(C) *If $ax_0 \ne 0$, $a = x_0^2$ and $b = 0$, then $x_n = x_0$ for all $n \ge 0$, and so $L(x_0;a,0;p) = 1$.*

(D) *If $ax_0 \ne 0$, $a \ne x_0^2$ and $b = 0$, then $x_{n+2} = x_n$ and $x_{n+1} \ne x_n$ for all $n \ge 0$, and so $L(x_0;a,0;p) = 2$.*

(E) *Let $f(x) = (x-\alpha)^2$ for some $\alpha \in \mathrm{GF}(p)$ (or equivalently, $b^2+4a = 0$). Then*

(1) *$L(\alpha;a,b;\mathrm{GF}(p)) = 1$,*

(2) *if $x_0 \ne \alpha$, then $X(x_0;a,b)$ contains 0 and $L(x_0;a,b;p) = p-1$.*

(F) *Let $f(x) = (x-\alpha)(x-\beta)$ for some $\alpha \ne \beta \in \mathrm{GF}(p^2)$.*

(1) *If* $f(x_0) = 0$, *then* $L(x_0; a, b; p) = 1$.
(2) *If* $p \neq 2$ *and* $\mathfrak{o}(m_f)$ *is even*, *then* $X(b/2; a, b)$ *contains* 0 *and* $L(b/2; a, b; p) = \mathfrak{o}(m_f) - 1$.
(3) *If* $p \neq 2$ *and* $\mathfrak{o}(m_f)$ *is odd*, *then* $X(b/2; a, b)$ *does not contain* 0 *and* $L(b/2; a, b; p) = \mathfrak{o}(m_f)$.
(4) *If* $f(x_0) \neq 0$, $x_0 \neq b/2$ *whenever* $p \neq 2$, *and the order* $\mathfrak{o}(M_f)$ *of the polynomial* $M_f(x) = x^2 - (2 + (b^2 + 4a)/f(x_0))x + 1$ *over* $\mathrm{GF}(p)$ *divides* $\mathfrak{o}(m_f)$ (*or equivalently*, $M_f(x)$ *divides* $x^{\mathfrak{o}(m_f)} - 1$), *then* $X(x_0; a, b)$ *contains* 0 *and* $L(x_0; a, b; p) = \mathfrak{o}(m_f) - 1$.
(5) *If* $f(x_0) \neq 0$, $x_0 \neq b/2$ *for* $p \neq 2$, *and* $\mathfrak{o}(M_f)$ *does not divide* $\mathfrak{o}(m_f)$, *then* $X(x_0; a, b)$ *does not contain* 0 *and* $L(x_0; a, b; p) = \mathfrak{o}(m_f)$.

Using this lemma, we are going to study all possible period lengths of sequences $X(x_0; a, b)$ with modulus m generated by the recursion (2) in Section 2 and all possible period lengths of sequences $X(x_0; a, b)$ with modulus m generated by the recursion (3) in Section 3.

2. Inversive congruential recursion. Let $m \geq 4$ be a fixed composite integer and let $m = p_1^{r_1} \ldots p_t^{r_t}$ be the prime factorization of m, where $t \geq 2$, $p_1, \ldots, p_t$ are distinct primes, and $r_1, \ldots, r_t$ are positive integers. For integers a, b, and x_0, let $X(x_0; a, b)$ be the sequence defined by the recursion (2) if it can be defined. As we have mentioned, every term of $X(x_0; a, b)$ must be relatively prime to m and the period length $L(x_0; a, b; m)$ of $X(x_0; a, b)$ with modulus m equals the least common multiple of the period lengths $L(x_0; a, b; p_i^{r_i})$ of $X(x_0; a, b)$ with moduli $p_i^{r_i}$, $1 \leq i \leq t$. We are going to consider first the sequence $X(x_0; a, b)$ with modulus a prime power p^k with $k \geq 2$. First, we have the following "well-defined" property.

LEMMA 2. *Let* p *be a prime*, *and let* k, a, b *and* x_0 *be integers with* $k \geq 2$. *Moreover*, *let* $f(x) = x^2 - bx - a$. *Then* a, b *and* x_0 *can be used to define an infinite sequence* $X(x_0; a, b)$ *with modulus* p^k *by the recursion* (2) *if and only if one of the following conditions holds*:

(A) $a \equiv 0 \bmod p$ *and* $\gcd(bx_0, p) = 1$.
(B) $\gcd(ax_0, p) = 1$ *and* $b \equiv 0 \bmod p$.
(C) $\gcd(abx_0, p) = 1$, $b \equiv 2x_0 \bmod p$, *and* $a \equiv -x_0^2 \bmod p$.
(D) $\gcd(abx_0(b^2 + 4a), p) = 1$ *and* $x_0^2 - x_0 b - a \equiv 0 \bmod p$.
(E) $p \neq 2$, $\gcd(ab(b^2 + 4a), p) = 1$, $x_0 \equiv b/2 \bmod p$, *and the order* $\mathfrak{o}(m_f)$ *of the polynomial* $m_f(x) = x^2 + (b^2/a + 2)x + 1$ *in* $\mathrm{GF}(p)[x]$ *is odd.*
(F) $\gcd(abx_0(b^2 + 4a)f(x_0), p) = 1$, $x_0 \not\equiv b/2 \bmod p$ *whenever* $p \neq 2$, *and the order* $\mathfrak{o}(M_f)$ *of* $M_f(x) = x^2 - (2 + (b^2 + 4a)/f(x_0))x + 1$ *in* $\mathrm{GF}(p)[x]$ *does not divide* $\mathfrak{o}(m_f)$.

Proof. As we have mentioned, a, b, and x_0 can be used to define an infinite sequence by the recursion (2) if and only if the sequence $X(x_0; a, b)$ with modulus p defined by the recursion (1) does not contain 0. From Lemma 1, the last statement holds if and only if $X(x_0; a, b)$ with modulus p is one of cases (A), (C), (D), (E)(1), and (F)(1), (3), and (5). In fact, with modulus p, Lemma 1(A) is case (A), both Lemma 1(C) and (D) together are case (B), Lemma 1(E)(1) is case (C), Lemma 1(F)(1) is case (D), Lemma 1(F)(3) is case (E), and Lemma 1(F)(5) is case (F).

The following two lemmas were obtained by Eichenauer-Herrmann and Topuzoğlu [7]. They are useful in describing the period length of the sequence $X(x_0; a, b)$ with modulus p^k for $k \geq 2$.

LEMMA 3 ([7], Lemma 6). *Let p be a prime and let k, a, b, and x_0 be integers with $k \geq 2$ and $\gcd(a, p) = 1$. Suppose that the sequence $X(x_0; a, b)$ can be defined by the recursion* (2). *Let λ_{k-1} and λ_k be the period length of $X(x_0; a, b)$ with modulus p^{k-1} and p^k, respectively. Then*

(A) $\lambda_k = \lambda_{k-1}$ *for* $x_{\lambda_{k-1}} \equiv x_0 \bmod p^k$.

(B) $\lambda_k = \mathfrak{o}(-ax_0^{-2})\lambda_{k-1}$ *for* $x_{\lambda_{k-1}} \not\equiv x_0 \bmod p^k$, $\lambda_{k-1} = 1$ *and* $\gcd(a + x_0^2, p) = 1$, *where* $\mathfrak{o}(-ax_0^{-2})$ *is the multiplicative order of* $-ax_0^{-2}$ *in* $\mathrm{GF}(p)$.

(C) $\lambda_k = p\lambda_{k-1}$ *for* $x_{\lambda_{k-1}} \not\equiv x_0 \bmod p^k$, *and either* $\lambda_{k-1} \geq 2$ *or* $\lambda_{k-1} = 1$ *and* $a \equiv -x_0^2 \bmod p$.

The following lemma is a little bit different from the original lemmas in [7].

LEMMA 4 ([7], Lemmas 7–9). *Let p be a prime and let k, a, b and x_0 be integers with $k \geq 2$ and $\gcd(a, p) = 1$. Suppose that the sequence $X(x_0; a, b)$ can be defined by the recursion* (2). *Let λ_{k-1} and λ_k be the period lengths of $X(x_0; a, b)$ with modulus p^{k-1} and p^k, respectively.*

(A) *If* $k \geq 3$ *and* $x_{\lambda_{k-1}} \not\equiv x_0 \bmod p^k$, *then* $x_{\lambda_k} \not\equiv x_0 \bmod p^{k+1}$.

(B) *If* $\lambda_1 \geq 2$ *and* $x_{\lambda_1} \not\equiv x_0 \bmod p^2$, *then* $x_{\lambda_2} \not\equiv x_0 \bmod p^3$.

(C) *If* $\lambda_1 = 1$, $a \equiv -x_0^2 \bmod p$, $x_1 \not\equiv x_0 \bmod p^2$ *and* $p \geq 5$, *then* $x_{\lambda_2} \not\equiv x_0 \bmod p^3$.

Proof. (B) and (C) are the same as Lemmas 8 and 9, respectively, in [7]. So, we prove (A) only. We follow the proof of Lemma 7 in [7] until we get the congruential equation

$$x_{\mu\lambda_{k-1}} \equiv x_0 + \mu(\alpha p^{k-1} + \beta p^k) + \Big(\sum_{1 \leq j \leq \mu-1} j\Big)\gamma\alpha p^k \bmod p^{k+1}, \tag{4}$$

where μ is any positive integer, α, β, and γ are some fixed integers with $\gcd(\alpha, p) = 1$ and $\gamma = 0$ if $p = 2$. If the conditions of Lemma 3(B) are satisfied, we take $\mu = \mathfrak{o}(-ax_0^{-2})$ and then the equation (4) becomes

$$x_{\lambda_k} \equiv x_0 + \mathfrak{o}(-ax_0^{-2})\alpha p^{k-1} + \Big(\mathfrak{o}(-ax_0^{-2})\beta + \Big(\sum_{1\le j\le \mu-1} j\Big)\gamma\alpha\Big)p^k$$
$$\not\equiv x_0 \bmod p^{k+1}$$

since $\gcd(\mathfrak{o}(-ax_0^{-2})\alpha, p) = 1$. If the conditions of Lemma 3(C) are satisfied, we take $\mu = p$ and then the equation (4) becomes $x_{\lambda_k} \equiv x_0 + \alpha p^k \not\equiv x_0 \bmod p^{k+1}$ since $\sum_{1\le j\le p-1} j \equiv 0 \bmod p$ if $p \ge 3$, and $\gamma = 0$ if $p = 2$. This completes the proof.

We are now ready to prove our main theorem of this section, which will describe all possible period lengths of the inversive congruential recursion with modulus p^k.

THEOREM 5. *Let p be a prime and let k, a, b and x_0 be integers with $k \ge 1$. Suppose that the sequence $X(x_0; a, b)$ with modulus p^k can be defined by the recursion* (2). *Let $f(x) = x^2 - bx - a$.*

(A) *If $a \equiv 0 \bmod p$ and $\gcd(bx_0, p) = 1$, then the period length $L(x_0; a, b; p^k) = 1$.*

(B) *Let $\gcd(ax_0, p) = 1$, $a \equiv x_0^2 \bmod p$, and $b \equiv 0 \bmod p$. Write $b = dp^j$ with $\gcd(d, p) = 1$ whenever $b \ne 0$. Also write $f(x_0) = cp^e$ with $\gcd(c, p) = 1$ when $f(x_0) \ne 0$.*

(1) *If either $f(x_0) = 0$ or $k \le e$, then $L(x_0; a, b; p^k) = 1$.*
(2) *If $k = e + 1$, then $L(x_0; a, b; p^k) = 2$.*
(3) *If $e + 1 < k$ and either $b = 0$ or $k \le j$, then $L(x_0; a, b; p^k) = 2$.*
(4) *If $k > e + 1$ and $k > j$, then $L(x_0; a, b; p^k) = 2p^{k-\max\{j,e+1\}}$.*

(C) *Let $\gcd(ax_0(a - x_0^2), p) = 1$ and $b \equiv 0 \bmod p$.*

(1) *If $b = 0$, then $L(x_0; a, b; p^k) = 2$.*
(2) *If $b = dp^j$ with $\gcd(d, p) = 1$, then $L(x_0; a, b; p^k) = 2$ if $1 \le k \le j$, and $L(x_0; a, b; p^k) = 2p^{k-j}$ if $k > j$.*

(D) *Let $\gcd(ab, p) = 1$, $b \equiv 2x_0 \bmod p$, and $a \equiv -x_0^2 \bmod p$. If $f(x_0) \ne 0$, write $f(x_0) = cp^e$ with $\gcd(c, p) = 1$.*

(1) *If either $f(x_0) = 0$ or $e \ge 2$ and $k \le e$, then $L(x_0; a, b; p^k) = 1$.*
(2) *If $k > e \ge 2$, then $L(x_0; a, b; p^k) = p^{k-e}$.*
(3) *If $p \ge 5$ and $e = 1$, then $L(x_0; a, b; p^k) = p^{k-1}$.*
(4) *Let $p = 3$ and $e = 1$. Write $a + b^2 = h3^s$ for some integer h with $\gcd(h, 3) = 1$ whenever $a + b^2 \ne 0$. Then $L(x_0; a, b; 3^k) = 3$ if either $a + b^2 = 0$ or $2 \le k \le s$, and $L(x_0; a, b; 3^k) = 3^{k-s+1}$ if $k \ge s + 1$.*

(E) *Let $\gcd(abx_0(b^2 + 4a), p) = 1$. Write $f(x_0) = cp^e$ with $\gcd(c, p) = 1$ whenever $f(x_0) \ne 0$.*

(1) *If either $f(x_0) = 0$ or $k \le e$, then $L(x_0; a, b; p^k) = 1$.*

(2) *If* $k > e \geq 2$, *then* $L(x_0; a, b; p^k) = \mathfrak{o}(-ax_0^{-2})p^{k-e-1}$.

(3) *Let* $k > e = 1$ *and write* $\mu = \mathfrak{o}(-ax_0^{-2})$. *Then* $L(x_0; a, b; p^k) = \mu$ *if* $x_\mu \equiv x_0 \bmod p^k$, *and* $L(x_0; a, b; p^k) = \mu p^{k-t+1}$ *if* t *is the smallest integer satisfying* $x_\mu \not\equiv x_0 \bmod p^t$ *and* $3 \leq t \leq k$.

(F) *Let* $\gcd(abx_0(b^2+4a)f(x_0), p) = 1$. *Suppose that either* $p > 2$, $x_0 \equiv b/2 \bmod p$ *and the order* $\lambda = \mathfrak{o}(m_f)$ *of* $m_f(x) = x^2 + (b^2/a + 2)x + 1$ *in* $\mathrm{GF}(p)[x]$ *is odd or the order* $\mathfrak{o}(M_f)$ *of the polynomial* $M_f(x) = x^2 - (2 + (b^2+4a)/f(x_0))x + 1$ *in* $\mathrm{GF}(p)[x]$ *does not divide* λ. *Then* p *is odd and* $L(x_0; a, b; p^k) = \lambda$ *if* $x_\lambda \equiv x_0 \bmod p^k$, *and* $L(x_0; a, b; p^k) = \lambda p^{k-t+1}$ *if* t *is the smallest positive integer satisfying* $x_\lambda \not\equiv x_0 \bmod p^t$ *and* $2 \leq t \leq k$.

Proof. Since a, b and x_0 can be used to define the infinite sequence $X(x_0; a, b)$ with modulus p^k by the recursion (2), we are going to prove this theorem according to all cases in Lemma 2.

(A) It is trivial for the case $a = 0$. So, consider $a \neq 0$ and write $a = rp^e$ with $\gcd(r, p) = 1$. Let s be the nonnegative integer satisfying $es < k \leq e(s+1)$. We are going to prove this case by induction on s.

Since $x_{n+1} \equiv p^e r x_n^{-1} + b \bmod p^t$, we have $L(x_0; a, b; p^t) = 1$ whenever $1 \leq t \leq e$. Suppose that for fixed integer $0 \leq s$, $L(x_0; a, b; p^t) = 1$ for each $es < t \leq e(s+1)$, or equivalently, there exists a positive integer w_s so that for any $es < t \leq e(s+1)$, $x_n \equiv u \bmod p^t$ is a constant for all $n \geq w_s$.

Now consider $e(s+1) < k \leq e(s+2)$. For any $n \geq w_s + 1$, $x_n \equiv p^e r x_{n-1}^{-1} + b \bmod p^k$. Since $n - 1 \geq w_s$, the term $x_{n-1} \equiv u \bmod p^{k-e}$ is a constant. So, $p^e r x_{n-1}^{-1} \equiv p^e r u^{-1} \bmod p^k$ is a constant. Therefore, $x_n \equiv p^e r x_{n-1}^{-1} + b \bmod p^k$ is a constant for all $n \geq w_s + 1$. Hence, $L(x_0; a, b; p^k) = 1$.

From now on, we consider $\gcd(a, p) = 1$. So, $X(x_0; a, b)$ with modulus p^k is purely periodic.

(B) From the definition, $x_1 \equiv x_0 \bmod p^k$ if and only if $f(x_0) = x_0^2 - bx_0 - a \equiv 0 \bmod p^k$. So, if $f(x_0) = 0$, then $L(x_0; a, b; p^k) = 1$. Now, we consider $f(x_0) \neq 0$.

If $k \leq e$, it is trivial that $L(x_0; a, b; p^k) = 1$. So, suppose $k > e$. Then $x_1 \not\equiv x_0 \bmod p^k$. If $k = e+1$ and p is odd, then, by Lemma 3(B), $L(x_0; a, b; p^{e+1}) = 2$ since $\mathfrak{o}(-ax_0^{-2}) = 2$. From Lemma 3(C), if p is even and $k = e+1$, then $L(x_0; a, b; p^{e+1}) = p = 2$.

Now, suppose $k > e + 1$. By the definition, $x_0 \equiv x_2 \bmod p^k$ if and only if $b^2 x_0 + ab + ax_0 \equiv x_0(bx_0 + a) \bmod p^k$. Simplifying the last congruential equation, $x_0 \equiv x_2 \bmod p^k$ if and only if $ab \equiv 0 \bmod p^k$. So, if either $b = 0$ or $k \leq j$, then $L(x_0; a, b; p^k) = 2$ by Lemma 3(A). If $k > j$, then $L(x_0; a, b; p^k) = 2p^{k-\max\{j, me+1\}}$ from Lemmas 3(C) and 4(A).

(C) From Lemma 1(D), $L(x_0; a, b; p) = 2$. By the definition, $x_2 \equiv a(ax_0^{-1} + b)^{-1} + b \bmod p^k$. If $b = 0$, it is trivial that $L(x_0; a, b; p^k) = 2$. Now suppose $b \neq 0$. After simplification, $x_2 \equiv x_0 \bmod p^k$ if and only if

$(a-x_0^2)b \equiv -x_0b^2 \bmod p^k$. The last congruential equation holds if and only if $1 \le k \le j$ since $b = dp^j$ and $\gcd(a-x_0^2, p) = 1$. So, $L(x_0; a, b; p^k) = 2$ if $1 \le k \le j$. Since $(a-x_0^2)b \not\equiv -x_0b^2 \bmod p^{j+1}$, $L(x_0; a, b; p^{j+1}) = 2p$ by Lemma 3(C). If $k > j$, then $L(x_0; a, b; p^k) = 2p^{k-j}$ by Lemmas 3(C) and 4(A) and (B).

(D) By Lemma 1(E)(1), $L(x_0; a, b; p) = 1$. From the definition, $x_1 \equiv x_0 \bmod p^k$ if and only if $f(x_0) = x_0^2 - bx_0 - a \equiv 0 \bmod p^k$. So, if either $f(x_0) = 0$ or $k \le e$, then $L(x_0; a, b; p^k) = 1$. Suppose $f(x_0) \ne 0$ and $k > e$. Since $a \equiv -x_0^2 \bmod p$, $L(x_0; a, b; p^{e+1}) = p$ by Lemma 3(C). If $e \ge 2$, then $L(x_0; a, b; p^k) = p^{k-e}$ by Lemmas 3(C) and 4(A).

Suppose now $e = 1$. From Lemmas 3(C) and 4(A) and (C), $L(x_0; a, b; p^k) = p^{k-1}$ if $p \ge 5$. So, suppose $p = 3$. It is trivial that $L(x_0; a, b; 9) = 3$. So, let $k \ge 3$. By the definition and a short calculation, $x_3 \equiv x_0 \bmod 3^k$ if and only if $af(x_0) \equiv -b^2f(x_0) \bmod 3^k$. The last congruential equality is equivalent to $a \equiv -b^2 \bmod 3^{k-1}$ since $f(x_0) = 3c$ with $\gcd(c, 3) = 1$. Since $b \equiv 2x_0 \bmod 3$ and $a \equiv -x_0^2 \bmod 3$, we have $a + b^2 \equiv 0 \bmod 3$. If $a + b^2 = 0$, then $L(x_0; a, b; 3^k) = 3$ by Lemmas 3(A). So, suppose $a + b^2 \ne 0$. If $s = 1$, then $L(x_0; a, b; 3^k) = 3^{k-1}$ by Lemmas 3(C) and 4(A). Suppose $s \ge 2$. If $k \le s$, then $L(x_0; a, b; 3^k) = 3$. If $k \ge s + 1$, then $L(x_0; a, b; 3^k) = 3^{k-s}$ by Lemmas 3(C) and 4(A).

(E) From the definition, $x_0 \equiv x_1 \bmod p^k$ if and only if $f(x_0) \equiv 0 \bmod p^k$. If either $f(x_0) = 0$ or $k \le e$, then $L(x_0; a, b; p^k) = 1$. If $k > e \ge 2$, then $L(x_0; a, b; p^k) = \mathfrak{o}(-ax_0^{-2})p^{k-e-1}$ from Lemmas 3(B), (C) and 4(A). Now suppose $e = 1$. By Lemma 3(B) again, $L(x_0; a, b; p^2) = \lambda = \mathfrak{o}(-ax_0^{-2})$. If $k > 2$ and $x_\lambda \equiv x_0 \bmod p^k$, then $L(x_0; a, b; p^k) = \lambda$. If $k > 2$ and if $3 \le t \le k$ is the smallest positive integer satisfying $x_\lambda \not\equiv x_0 \bmod p^t$, then $L(x_0; a, b; p^k) = \mathfrak{o}(-ax_0^{-2})p^{k-t+1}$ by Lemmas 3(B), (C) and 4(A).

(F) Under the assumption $\gcd(ab, p) = 1$, the only case for $p = 2$ is that $a \equiv 1 \equiv b \bmod 2$. In this case, $\mathfrak{o}(m_f)$ is 3 and so $L(x_0; a, b; 2) = 2$. This implies that the sequence $X(x_0; a, b)$ with modulus 2 contains 0; a contradiction. So, p is odd.

From Lemma 1(F)(3) and (5), $L(x_0; a, b; p) = \lambda = \mathfrak{o}(m_f)$. If $x_\lambda \equiv x_0 \bmod p^k$, then $L(x_0; a, b; p^k) = \mathfrak{o}(m_f)$ by Lemma 3(A). If $2 \le t \le k$ is the smallest integer satisfying $x_\lambda \not\equiv x_0 \bmod p^e$, then $L(x_0; a, b; p^k) = \mathfrak{o}(m_f)p^{k-t+1}$ by Lemmas 3(A), (C), 4(A) and (B). This completes the proof of this theorem.

The case Theorem 5(B)(3) with $j = 1 = e$ is consistent with the result obtained by Eichenauer, Lehn, and Topuzoğlu [4]. Also, cases (D)(4), (D)(5) with $s = 1$, and (F) in Theorem 5 are consistent with results obtained by Eichenauer-Herrmann and Topuzoğlu [7]. Also, we have given conditions $x_\lambda \equiv x_0$ and $x_\lambda \not\equiv x_0$ modulo a prime power in both cases Theorem 5(E)(3) and (F), respectively. We are going to modify these two conditions. First, we need the following

LEMMA 6. *Let p be a prime and let k, a, b, and x_0 be integers with $k \geq 2$. Suppose that the sequence $X(x_0; a, b) : x_0, x_1, x_2, \ldots$ with modulus p^k can be defined by the recursion* (2). *Let $U(1, x_0; a, b) : u_0, u_1, u_2, \ldots$ be the linear recurrence sequence of integers defined by $u_0 = 1$, $u_1 = x_0$, and $u_{n+2} = bu_{n+1} + au_n$ for all $n \geq 0$. Then $\gcd(u_n, p) = 1$ and $x_n \equiv u_{n+1}/u_n \bmod p^k$ for all $n \geq 0$.*

Proof. From the definition, x_n is not congruent to 0 modulo p for all $n \geq 0$. So, $\gcd(u_n, p) = 1$ by Lemma 1. Since $x_0 \equiv u_1 \equiv u_1/u_0 \bmod p^k$ and $u_{n+2} \equiv bu_{n+1} + au_n \bmod p^k$, the result $x_n \equiv u_{n+1}/u_n \bmod p^k$ can be proved by induction on n.

The following theorem is a modification of the case Theorem 5(E)(3).

THEOREM 7. *Let p be an odd prime and let k, a, b and x_0 be integers so that $k \geq 2$, $\gcd(abx_0(b^2 + 4a), p) = 1$ and $x_0^2 - bx_0 - a = cp$ for some integer c with $\gcd(c, p) = 1$. Write $(ax_0^{-1})^{p-1} - x_0^{p-1} \equiv \upsilon p \bmod p^2$ for some integer υ, where x_0^{-1} is the multiplicative inverse of x_0 modulo p^2.*

(A) *If $\gcd(c + 2^{-1}\upsilon(x_0^2 + a), p) = 1$, then $L(x_0; a, b; p^k) = \mathfrak{o}(-ax_0^{-2})p^{k-2}$, where 2^{-1} is the multiplicative inverse of 2 modulo p.*

(B) *If $c \equiv -\upsilon(x_0^2 + a)/2 \bmod p$, then $L(x_0; a, b; p^3) = \mathfrak{o}(-ax_0^{-2})$ and, whenever $k \geq 4$, there is exactly one integer $0 \leq d < p^{k-3}$ so that $L(x_0; a, b + dp^2; p^k) = \mathfrak{o}(-ax_0^{-2})$.*

Proof. We already know that $L(x_0; a, b; p) = 1$ and $L(x_0; a, b; p^2) = \mathfrak{o}(-ax_0^{-2}) = \lambda$ by Theorem 5(E)(3). Now, we consider the sequence $X(x_0; a, b)$ with modulus p^3.

Since $\gcd(ax_0, p) = 1$, there is an integer β so that $\beta x_0 \equiv -a \bmod p^3$. Write $x_0 = \alpha$. Let $b_c = \beta + \alpha$ and $g(x) = x^2 - b_c x - a$. So, $g(x_0) \equiv 0 \bmod p^3$. Moreover, $b - b_c \equiv x_0^{-1}cp \bmod p^3$ since $f(x_0) = x_0^2 - bx_0 - a = cp$. Consider two corresponding linear recurrence sequences $U(1, x_0; a, b) : u_0, u_1, \ldots$ and $U(1, x_0; a, b_c) : u_{c,0}, u_{c,1}, \ldots$ defined as in Lemma 6, respectively. By Lemma 6, $x_n \equiv u_{n+1}/u_n \bmod p^3$ for all $n \geq 0$. Furthermore, it can be shown by induction on n that $u_{c,n} \equiv \alpha^n \bmod p^3$ for all $n \geq 0$. Now, let $W(0, 1; a, b_c) : \omega_{c,0}, \omega_{c,1}, \ldots$ be the linear recurrence sequence defined by $\omega_{c,0} = 0$, $\omega_{c,1} = 1$, and $\omega_{c,n+2} = b_c\omega_{c,n+1} + a\omega_{c,n}$ for all $n \geq 0$. Since $\alpha \not\equiv \beta \bmod p$ from $\gcd(b^2 + 4a, p) = 1$, one can show by induction on n that $\omega_{c,n} \equiv (\alpha^n - \beta^n)/(\alpha - \beta) \bmod p^3$ for all $n \geq 0$.

It is easy to see from the definition that $u_0 \equiv u_{c,0}$, $u_1 \equiv u_{c,1}$, $u_2 \equiv u_{c,2} + \omega_{c,1}u_{c,1}x_0^{-1}cp$ and $u_3 \equiv u_{c,3} + (\omega_{c,1}u_{c,2} + \omega_{c,2}u_{c,1})x_0^{-1}cp + \omega_{c,1}u_{c,1}(x_0^{-1}cp)^2 \bmod p^3$. Let $\sigma_n = \sum_{1 \leq j \leq n-1} \omega_{c,j}u_{c,n-j}$ and $\tau_n = \sum_{1 \leq j \leq n-2} \omega_{c,j}\sigma_{n-j}$ for all $n \geq 3$, and let $\sigma_2 = \omega_{c,1}u_{c,1}$. One can show by induction on n that

$u_n \equiv u_{c,n} + \sigma_n x_0^{-1}cp + \tau_n(x_0^{-1}cp)^2 \bmod p^3$ for all $n \geq 3$. Since $\omega_{c,n} \equiv (\alpha^n - \beta^n)/(\alpha-\beta)$ and $u_{c,n} \equiv \alpha^n \bmod p^3$, we have, after a short computation,

$$\begin{aligned}(5)\qquad \sigma_n &= \sum_{1\le j\le n-1} \omega_{c,j}u_{c,n-j} \equiv \Big(\sum_{0\le j\le n-1} \alpha^{n-j}(\alpha^j - \beta^j)\Big)/(\alpha-\beta)\\ &\equiv n\alpha^n/(\alpha-\beta) - \alpha(\alpha^n-\beta^n)/(\alpha-\beta)^2 \bmod p^3\end{aligned}$$

and

$$\begin{aligned}(6)\quad \tau_n &= \sum_{1\le j\le n-2} \omega_{c,j}\sigma_{n-j}\\ &\equiv (\alpha-\beta)^{-2}\Big(\sum_{0\le j\le n-2} (\alpha^j-\beta^j)(n-j)\alpha^{n-j}\Big)\\ &\quad - \alpha(\alpha-\beta)^{-3}\Big(\sum_{0\le j\le n-2} (\alpha^j-\beta^j)(\alpha^{n-j}-\beta^{n-j})\Big)\\ &\equiv (\alpha-\beta)^{-2}((n+2)(n-1)\alpha^n/2 - n\alpha^2(\alpha^{n-1}-\beta^{n-1})/(\alpha-\beta)\\ &\quad + ((n-2)\alpha^2\beta^n - (n-1)\alpha^3\beta^{n-1} + \alpha^{n+1}\beta)/(\alpha-\beta)^2)\\ &\quad - \alpha(\alpha-\beta)^{-3}((n-1)\alpha^n - \beta^2(\alpha^{n-1}-\beta^{n-1})/(\alpha-\beta)\\ &\quad - \alpha^2(\alpha^{n-1}-\beta^{n-1})/(\alpha-\beta) + (n-1)\beta^n) \bmod p^3.\end{aligned}$$

Since $\beta x_0 \equiv -a \bmod p^3$, we have $-ax_0^{-2} \equiv \alpha\beta^{-1} \bmod p$. This implies $\mathfrak{o}(-ax_0^{-2}) = \mathfrak{o}(m_f) = \lambda$. So, $\beta^\lambda \equiv \alpha^\lambda \bmod p$. Hence, $\alpha^{p-1} \equiv \beta^{p-1} \bmod p$. Write $\beta^{p-1} \equiv \alpha^{p-1} + \upsilon p \bmod p^2$ for some integer υ. Note that $x_0 \equiv x_\lambda \bmod p^3$ if and only if $x_0 \equiv x_{p-1} \bmod p^3$ by Lemma 3(C). So, we consider x_{p-1} instead of x_λ. By formula (5) and (6) and simplification,

$$\begin{aligned}&(x_0^{-1}cp)\sigma_{p-1}\\ &\quad\equiv -\alpha^{p-1}(\alpha-\beta)^{-1}(x_0^{-1}cp) + ((\alpha-\beta)^{-1} + \alpha\upsilon(\alpha-\beta)^{-2})x_0^{-1}cp^2 \bmod p^3,\\ &(x_0^{-1}cp)\sigma_p\\ &\quad\equiv -\alpha^p(\alpha-\beta)^{-1}(x_0^{-1}cp) + (\alpha(\alpha-\beta)^{-1} + \alpha\beta\upsilon(\alpha-\beta)^{-2})x_0^{-1}cp^2 \bmod p^3,\end{aligned}$$

$$(x_0^{-1}cp)^2\tau_{p-1} \equiv 3\alpha(\alpha-\beta)^{-3}(x_0^{-1}cp)^2 \bmod p^3,$$

and

$$(x_0^{-1}cp)^2\tau_p \equiv (\alpha^2+2\alpha\beta)(\alpha-\beta)^{-3}(x_0^{-1}cp)^2 \bmod p^3.$$

By Lemma 6 and a short computation, we have

$$\begin{aligned}x_{p-1} &\equiv u_p/u_{p-1}\\ &\equiv (u_{c,p} + \sigma_p x_0^{-1}cp + \sigma_p(x_0^{-1}cp)^2)/(u_{c,p-1} + \sigma_{p-1}x_0^{-1}cp + \sigma_{p-1}(x_0^{-1}cp)^2)\\ &\equiv \alpha + (-\upsilon c(\alpha-\beta)^{-1} - 2c^2\alpha^{-1}(\alpha-\beta)^{-2})p^2 \bmod p^3.\end{aligned}$$

Since $x_0 = \alpha$, $x_{p-1} \equiv x_0 \bmod p^3$ if and only if $0 \equiv -\upsilon c(\alpha-\beta)^{-1} - 2c^2\alpha^{-1}(\alpha-\beta)^{-2} \bmod p$. The last congruential equality is equivalent to

$c \equiv -v\alpha(\alpha-\beta)/2 \equiv -v(x_0^2+a)/2 \bmod p$. By Lemmas 3(C) and 4(A), if $\gcd(c+v(x_0^2+a),p)=1$, then $L(x_0;a,b;p^3)=\mathfrak{o}(-ax_0^{-2})p$, and so $L(x_0;a,b;p^k)=\mathfrak{o}(-ax_0^{-2})p^{k-2}$ for all $k\ge 3$.

Suppose $c \equiv -v(x_0^2+a)/2 \bmod p$. Then $\gcd(v,p)=1$ since $\gcd(c(x_0^2+a),p)=1$. Note that $L(x_0;a,b;p^3)=\mathfrak{o}(-ax_0^{-2})$ from Lemma 3(A). Assume $k>3$ and let $3\le t<k$ be any integer satisfying $L(x_0;a,b;p^i)=\mathfrak{o}(-ax_0^{-2})$ for all $2\le i\le t$. Write $x_{p-1}\equiv x_0+\xi p^t \bmod p^{t+1}$. Take any integer $0\le d<p$ and consider the sequence $X(x_0;a,b+dp^{t-1}): x_{d,0},x_{d,1},\ldots$ with modulus p^{t+1}. Consider the corresponding linear recurrence sequence $U(1,x_0;a,b+dp^{t-1}): u_{d,0},u_{d,1},\ldots$ By Lemma 6, $x_{d,n}\equiv u_{d,n+1}/u_{d,n} \bmod p^{t+1}$ for all $n\ge 0$. Let $W(0,1;a,b): w_0,w_1,\ldots$ be the linear recurrence sequence defined by $w_0=0$, $w_1=1$, and $w_{n+2}=bw_{n+1}+aw_n$ for all $n\ge 0$. By similar arguments, one can show by induction on n that for all $n\ge 2$,

$$u_{d,n}\equiv u_n+\sum_{1\le j\le n-1} w_j u_{n-j} dp^{t-1} \bmod p^{t+1}. \tag{7}$$

It is easy to show by induction on n that $w_1\equiv \omega_{c,1}$ and $w_n\equiv\omega_{c,n}+(\sum_{1\le j\le n-1}\omega_{c,j}\omega_{c,n-j})x_0^{-1}cp \bmod p^2$ for all $n\ge 2$. Since $u_1\equiv u_{c,1}$ and $u_n\equiv u_{c,n}+\sigma_n x_0^{-1}cp \bmod p^2$ for all $n\ge 2$, (7) becomes, for all $n\ge 3$,

$$\begin{aligned}u_{d,n}&\equiv u_n+\sum_{1\le j\le n-1}\omega_{c,j}u_{n-j}dp^{t-1}\\&\quad+\sum_{2\le j\le n-1}u_{n-j}\Big(\sum_{1\le i\le j-1}\omega_{c,i}\omega_{c,j-i}\Big)x_0^{-1}cdp^t\\&\equiv u_n+\sum_{1\le j\le n-1}\omega_{c,j}u_{c,n-j}dp^{t-1}+\sum_{1\le j\le n-2}\omega_{c,j}\sigma_{n-j}x_0^{-1}cdp^t\\&\quad+\sum_{2\le j\le n-1}u_{n-j}\Big(\sum_{1\le i\le j-1}\omega_{c,i}\omega_{c,j-i}\Big)x_0^{-1}cdp^t \bmod p^{t+1}.\end{aligned}\tag{8}$$

Let $\chi_n=\sum_{2\le j\le n-1}u_{n-j}(\sum_{1\le i\le j-1}\omega_{c,i}\omega_{c,n-i})$ for all $n\ge 3$. From the definitions of σ_n and τ_n, (8) can be rewritten as

$$u_{d,n}\equiv u_n+\sigma_n dp^{t-1}+(\tau_n+\chi_n)x_0^{-1}cdp^t \bmod p^{t+1} \qquad \text{for all } n\ge 3.$$

Since $u_n\equiv u_{c,n} \bmod p$ for all $n\ge 0$, we have

$$\begin{aligned}\chi_n&=\sum_{2\le j\le n-1}u_{n-j}\Big(\sum_{1\le i\le j-1}\omega_{c,i}\omega_{c,j-i}\Big)\\&\equiv(n+1)(n-2)\alpha^n 2^{-1}(\alpha-\beta)^{-2}\\&\quad+((n-1)\alpha\beta^{n+1}-n\alpha^2\beta^n+2\alpha^n\beta^2-\alpha^{n-1}\beta^3)(\alpha-\beta)^{-4}\\&\quad-(n-2)\alpha^n(\alpha+\beta)(\alpha-\beta)^{-3}\\&\quad+(\alpha\beta^n-\alpha^{n-1}\beta^2)(\alpha+\beta)(\alpha-\beta)^{-4} \bmod p\end{aligned}$$

for all $n \geq 3$. Therefore,

$$u_{d,p-1} \equiv u_{p-1} - \alpha^{p-1}(\alpha-\beta)^{-1}dp^{t-1} + ((\alpha-\beta)^{-1} + \alpha\upsilon(\alpha-\beta)^{-2})dp^t + (8\alpha^2 + 4\alpha\beta + 2\beta^2)\alpha^{-1}(\alpha-\beta)^{-3}x_0^{-1}cdp^t \bmod p^{t+1},$$

and

$$u_{d,p} \equiv u_p - \alpha^p(\alpha-\beta)^{-1}dp^{t-1} + (\alpha(\alpha-\beta)^{-1} + \alpha\beta\upsilon(\alpha-\beta)^{-2})dp^t + (2\alpha^2 + 6\alpha\beta + 2\beta^2)(\alpha-\beta)^{-3}x_0^{-1}cdp^t \bmod p^{t+1}.$$

Since $x_{p-1} \equiv x_0 + \xi p^t \bmod p^{t+1}$ and $u_{p-1} \equiv \alpha^{p-1} \equiv 1$, $x_0 \equiv \alpha$, and $c \equiv -\upsilon\alpha(\alpha-\beta)/2 \bmod p$, we have $x_{d,p-1} \equiv u_{d,p}/u_{d,p-1} \equiv x_0 + (\xi + 2\alpha^2\upsilon(\alpha-\beta)^{-2}d)p^t \bmod p^{t+1}$. This implies that $x_{d,p-1} \equiv x_{d,0} \equiv x_0 \bmod p^{t+1}$ if and only if $d \equiv -\xi(\alpha-\beta)^2/(2\alpha^2\upsilon) \bmod p$. Since $(\alpha-\beta)^2 \equiv b^2 + 4a \bmod p$, $x_{d,p-1} \equiv x_{d,0} \bmod p^{t+1}$ if and only if $d \equiv -\xi(b^2+4a)/(2x_0^2\upsilon) \bmod p$. We have shown that there is exactly one integer $0 \leq d < p$ so that $L(x_0; a, b + dp^{t-1}; p^{t+1}) = \mathfrak{o}(-ax_0^{-2})$ whenever $L(x_0; a, b; p^t) = \mathfrak{o}(-ax_0^{-2})$. Case (B) of this theorem holds by taking such d repeatedly starting from $t = 2$. This completes the proof.

The following theorem modifies Theorem 5(F).

THEOREM 8. *Let $p > 2$ and $\gcd(ab(b^2+4a)(x_0^2 - bx_0 - a), p) = 1$. Suppose that either $x_0 \equiv b/2 \bmod p$ and the order $\lambda = \mathfrak{o}(m_f)$ of $m_f(x) = x^2 + (b^2/a + 2)x + 1$ in $\mathrm{GF}(p)[x]$ is odd or $x_0 \not\equiv b/2 \bmod p$ and the order $\mathfrak{o}(M_f)$ of $M_f(x) = x^2 - (2 + (b^2+4a)/f(x_0))x + 1$ in $\mathrm{GF}(p)[x]$ does not divide $\mathfrak{o}(m_f)$. Let $k \geq 2$.*

(A) *If $L(x_0; a, b; p^{k-1}) = \mathfrak{o}(m_f)$, then there exists exactly one integer $0 \leq d < p^{k-2}$ such that $L(x_0; a, b + dp; p^k) = \mathfrak{o}(m_f)$.*

(B) *If $x_\lambda \equiv x_0 + \upsilon p \bmod p^2$ for some integer $0 \leq \upsilon < p$, then $L(x_0; a, b + dp; p^2) = \mathfrak{o}(m_f)$ if and only if $d \equiv \upsilon(b^2+4a)/2\lambda(x_0^2 - bx_0 - a) \bmod p$.*

Proof. Let d be any integer. As in the proof of the last theorem, consider the sequences $X(x_0; a, b) : x_0, x_1, \ldots$ and $X(x_0; a, b + dp^{k-1}) : x_{d,0}, x_{d,1}, \ldots$ with modulus p^k and their corresponding linear recurrence sequences $U(1, x_0; a, b) : u_0, u_1, \ldots$ and $U(1, x_0; a, b + dp^{k-1}) : u_{d,0}, u_{d,1}, \ldots$, respectively. From Lemma 6, $x_n \equiv u_{n+1}/u_n$ and $x_{d,n} \equiv u_{d,n+1}/u_{d,n} \bmod p^k$ for all $n \geq 0$. Moreover, let $W(0, 1; a, b) : w_0, w_1, w_2, \ldots$ be the same linear recurrence sequence as in the proof of Theorem 7. One can show by induction on n that for all $n \geq 2$,

$$u_{d,n} \equiv u_n + \sum_{1 \leq j \leq n-1} w_j u_{n-j} dp^{k-1} \bmod p^k. \tag{9}$$

Note that $f(x) = x^2 - bx - a$ is the characteristic polynomial for both sequences $U(1, x_0; a, b)$ and $W(0, 1; a, b)$ with modulus p (or equivalently, over $\mathrm{GF}(p)$). Since $\gcd(b^2 + 4a, p) = 1$, $f(x)$ is not a square in $\mathrm{GF}(p)[x]$.

Let $\alpha, \beta \in \mathrm{GF}(p^2)$ be the roots of $f(x)$. It is easy to see that for all $n \geq 0$, $u_n = ((x_0-\beta)\alpha^n + (\alpha - x_0)\beta^n)/(\alpha-\beta)$ in $\mathrm{GF}(p^2)$. In particular, $u_\lambda = \alpha^\lambda$ in $\mathrm{GF}(p^2)$ where $\lambda = \mathfrak{o}(m_f)$. It can also be shown by induction on n that for all $n \geq 0$, $w_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ in $\mathrm{GF}(p^2)$. So, in $\mathrm{GF}(p^2)$,

$$\begin{aligned}\sum_{1\le j\le n-1} w_j u_{n-j} = &\sum_{0\le j\le n-1} ((x_0-\beta)\alpha^n + (\alpha-x_0)\beta^n(\alpha\beta^{-1})^j \\ &\quad - (x_0-\beta)\alpha^n(\alpha^{-1}\beta)^j - (\alpha-x_0)\beta^n)(\alpha-\beta)^{-2} \\ = &\,(n(x_0-\beta)\alpha^n + (\alpha-x_0)\beta(\alpha^n-\beta^n)(\alpha-\beta)^{-1} \\ &\quad - (x_0-\beta)\alpha(\alpha^n-\beta^n)(\alpha-\beta)^{-1} - n(\alpha-x_0)\beta^n)(\alpha-\beta)^{-2}\end{aligned}$$

for all $n \geq 2$. In particular,

$$\sum_{1\le j\le \lambda-1} w_j u_{\lambda-j} = \lambda\alpha^\lambda(2x_0-\beta-\alpha)(\alpha-\beta)^{-2} \tag{10}$$

and

$$\sum_{1\le j\le \lambda} w_j u_{\lambda-j+1} = \lambda\alpha^\lambda(x_0\alpha + x_0\beta - 2\alpha\beta)(\alpha-\beta)^{-2}. \tag{11}$$

Note that both values in (10) and (11) are in $\mathrm{GF}(p)$, and so can be viewed as an integer modulo p. Since $x_\lambda \equiv x_0 \bmod p^{k-1}$, we can write $x_\lambda \equiv x_0 + \upsilon p^{k-1} \bmod p^k$ for some integer $0 \leq \upsilon < p$. So, $u_{\lambda+1} \equiv u_\lambda x_0 + \alpha^\lambda \upsilon p^{k-1} \bmod p^k$. Using this result and formulas (9)–(11), we have

$$\begin{aligned}x_{d,\lambda} &\equiv u_{d,\lambda+1}/u_{d,\lambda} \equiv x_0 + (\upsilon - 2d\lambda(x_0^2 - (\alpha+\beta)x_0 + 2\alpha\beta)(\alpha-\beta)^{-2})p^{k-1} \\ &\equiv x_0 + (\upsilon - 2d\lambda(x_0^2 - bx_0 - a)/(b^2+4a))p^{k-1} \bmod p^k.\end{aligned}$$

Therefore, $x_{d,\lambda} \equiv x_0 \bmod p^k$ if and only if $d \equiv \upsilon(b^2+4a)/(2\lambda(x_0^2 - bx_0 - a)) \bmod p$. Since $\gcd(2\lambda(x_0^2 - bx_0 - a), p) = 1$, such a d exists uniquely when we consider $0 \leq d < p$. This theorem is obtained by taking such d repeatedly starting from $k = 2$.

Note that the result of Theorem 8(B) is consistent with the result obtained by Eichenauer-Herrmann [6]. The following result is an easy application of Theorem 5, which is consistent with results obtained by Huber [9]. We will use the usual notation $p^t \,\|\, m$ for $p^t \mid m$ but $p^{t+1} \nmid m$.

Corollary 9. *Let $m > 1$ be a composite integer and let a, b and x_0 be integers so that the infinite sequence $X(x_0; a, b)$ with modulus m can be defined by the recursion* (2). *Then $X(x_0; a, b)$ has the maximal period length among all inversive congruential pseudorandom number generators with modulus m if and only if for any prime divisor of m one of the following conditions holds*:

(A) $2^t \,\|\, m$, $\gcd(ax_0, 2) = 1$ *and either* $b \equiv 0 \bmod 2$ *when* $t = 1$ *or* $a \equiv 1 \bmod 4$, $b \equiv 2 \bmod 4$, *and* $x_0 \equiv 1 \bmod 2$ *when* $t \geq 2$.

(B) $p^t \parallel m$ *with* p *odd*, $\gcd(abx_0(b^2+4a)(x_0^2-bx_0-a),p)=1$, *the order* $\lambda=\mathfrak{o}(m_f)$ *of the polynomial* $m_f(x)=x^2+(b^2/a+2)x+1$ *in* $\mathrm{GF}(p)[x]$ *equals* $(p+1)/2, x_{(p+1)/2}\not\equiv x_0 \bmod p^2$ *whenever* $t\ge 2$, *and either* $x_0\equiv b/2 \bmod p$ *and* $p\equiv 1 \bmod 4$ *or* $x_0 \not\equiv b/2 \bmod p$ *and the order* $\mathfrak{o}(M_f)$ *of* $M_f(x)=x^2-(2+(b^2+4a)/f(x_0))x+1$ *in* $\mathrm{GF}(p)[x]$ *does not divide* $(p+1)/2$.

Proof. Note that the infinite sequence $X(x_0;a,b)$ with modulus m has the maximal period length among all inversive congruential pseudorandom number generators with modulus m if and only if for any prime factor p of m, $X(x_0;a,b)$ with modulus p^t has the maximal period length among all inversive congruential pseudorandom number generators with modulus p^t, where $p^t \parallel m$.

Let $2^t \parallel m$. Then $\gcd(x_0,2)=1$. From Theorem 5, the cases we have to consider are either $a\equiv 0$ or $b\equiv 0 \bmod 2$, but not both. If $t=1$, the sequence $X(x_0;a,b)$ with modulus 2 having the maximal period length among all inversive congruential pseudorandom number generators with modulus 2 if and only if $\gcd(ax_0,2)=1$ and $b\equiv 0 \bmod 2$. If $t\ge 2$, $X(x_0;a,b)$ with modulus 2^t has the maximal period length among all inversive congruential pseudorandom number generators with modulus 2^t if and only if the case Theorem 5(B)(4) holds. This proves (A).

Let $p^t \parallel m$ with p odd. Note that if either $L(x_0;a,b;p)=p-1$ or $L(x_0;a,b;p)=p+1$, then $X(x_0;a,b)$ with modulus p contains 0. So, the sequence $X(x_0;a,b)$ with modulus p having the maximal period length among all inversive congruential pseudorandom number generators with modulus p if and only if $L(x_0;a,b;p)=(p+1)/2$, because $L(x_0;a,b;p)$ divides either $p-1$ or $p+1$ by Theorem 5. The last statement holds if and only if it is the case Theorem 5(F) together with $x_\lambda \not\equiv x_0 \bmod p^2$ when $t\ge 2$. This completes the proof.

Let m be a composite positive integer and let $m=p_1^{r_1}\dots p_t^{r_t}$ be the prime factorization of m, where $p_1,\dots,p_t$ are distinct primes and $r_1,\dots,r_t$ are positive integers. To get a sequence with modulus m having the maximal period length, we can first take a sequence $X(x_{i,0};a_i,b_i)$ with each modulus $p_i^{r_i}$, $1\le i\le t$, satisfying conditions (A) or (B) of Corollary 9, and then use the Chinese Remainder Theorem to get a sequence $X(x_0;a,b)$ with modulus m. If $p=2$ is a prime divisor of m, it is easy to use the condition (A) of Corollary 9 to get the desired sequence with modulus a power of 2. If p is an odd prime factor of m, we have to do much more work.

Let p be an odd prime and k be a positive integer. To get a sequence $X(x_0;a,b)$ with modulus p^k which satisfies the condition (B) of Corollary 9, we have first to find numbers a and b so that the order of the polynomial $m_f(x)=x^2+(b^2/a+2)x+1$ in $\mathrm{GF}(p)[x]$ is $(p+1)/2$. We can pick up suitable a and b in the following way.

Note that Chou [1] gave several methods to find polynomials over $\mathrm{GF}(p)$ of order $p+1$. We can first use his methods to find a polynomial $m(x) = x^2 - cx + 1$, $0 \le c < p$, of order $p+1$ in $\mathrm{GF}(p)[x]$. Consider the sequence $v_0, v_1, \ldots$ defined by $v_0 = 2$, $v_1 = c$, and $v_{n+2} = cv_{n+1} - v_n$ for all $n \ge 0$. Then $v_n = \alpha^n + \alpha^{pn}$ for all $n \ge 0$, where α is a root of $m(x)$ in $\mathrm{GF}(p^2)$. So, $c^2 - 2 = v_2 = \alpha^2 + \alpha^{2p}$ in $\mathrm{GF}(p^2)$. Since $m(x)$ is of order $p+1$, $m_f(x) = x^2 - v_2 x + 1$ is of order $(p+1)/2$ in $\mathrm{GF}(p)[x]$. From the relation $c \equiv -b^2/a - 2 \bmod p$, we can get $p-1$ desired pairs of numbers a and b which are not congruent to $0 \bmod p$.

Once we have suitable numbers a and b, we can choose a suitable number x_0 as follows. Note that the period length of the sequence $v_0, v_1, \ldots$ over $\mathrm{GF}(p)$ is $p+1$. Any polynomial $x^2 - dx + 1$ over $\mathrm{GF}(p)$ is of order $(p+1)/2$ if and only if $d \equiv v_{2n}$ for some positive integer n satisfying $\gcd(n, (p+1)/2) = 1$. Take any integer w so that $w \not\equiv v_{2n} \bmod p$ for any integer $0 \le n < (p+1)/2$. Then the order of $M_f(x) = x^2 - wx + 1$ in $\mathrm{GF}(p)[x]$ does not divide $(p+1)/2$. Let $t \equiv (b^2 + 4a)/(w-2) \bmod p$. If the congruential equation $x^2 - bx + a \equiv t \bmod p$ does not have a solution, we pick up another w and then find a new t and solve this new congruential equation. Suppose that the last congruential equation has a solution, say x_0. If $k = 1$, the sequence $X(x_0; a, b)$ is as required. If $k \ge 2$, we check the condition $x_{(p+1)/2} \not\equiv x_0 \bmod p^2$. If the condition is satisfied, we are done; otherwise, the sequences $X(x_0 + cp; a, b)$, $1 \le c < p$, are as desired.

3. Generalized inversive congruential recursion. Let p be a prime and k be a positive integer again. In this section, we are going to study the sequence $X(x_0; a, b)$ with modulus p^k which is defined by the recursion (3). Let $L_G(x_0; a, b; p^k)$ be the period length of the sequence $X(x_0; a, b)$ with modulus p^k which is defined by the recursion (3). As we have mentioned in Section 1, if $X(x_0; a, b)$ with modulus p does not contain 0, then $L_G(x_0; a, b; p^k) = L(x_0; a, b; p^k)$. So, if $X(x_0; a, b)$ with modulus p does not contain 0, then $L_G(x_0; a, b; p^k)$ must be one of the cases in Theorem 5. Hence, we will concentrate on the case where $X(x_0; a, b)$ with modulus p contains 0. We need the following lemma.

LEMMA 10. *Let p be a prime and k be a positive integer so that either $k \ge 1$ if p is odd or $k \ge 3$ if $p = 2$. Let a, b and x_0 be integers and let the sequence $X(x_0; a, b) : x_0, x_1, \ldots$ with modulus p^k be defined by the recursion* (3). *If there is a nonnegative integer t so that $x_t \equiv 0 \bmod p$, then $x_{t+1} \equiv b \bmod p^k$.*

Proof. Write $\mu = \phi(p^k) = (p-1)p^{k-1}$ and $x_t \equiv rp \bmod p^k$ for some integer r. Then we have $x_{t+1} \equiv a(rp)^{\mu-1} + b \bmod p^k$. Note that $\mu - 1 =$

$(p-1)p^{k-1}-1 \geq k$ if either $k \geq 1$ when p is odd or $k \geq 3$ when $p=2$. So, $x_{t+1} \equiv a(cp)^{\mu-1}+b \equiv b \bmod p^k$.

Using this lemma, we can prove the following theorem which will list all possible period lengths of sequences with modulus p^k defined by the recursion (3) and containing 0 with modulus p.

THEOREM 11. *Let p be a prime and $k \geq 2$ be a positive integer. Let a, b and x_0 be integers, and let the sequence $X(x_0;a,b) : x_0, x_1, \ldots$ with modulus p^k be defined by the recursion* (3). *Moreover, suppose the sequence $X(x_0;a,b)$ with modulus p contains* 0.

(A) *If $a \equiv 0 \bmod p$ and either $b \equiv 0 \bmod p$ or $x_0 \equiv 0 \bmod p$, then $L_G(x_0;a,b;p^k)=1$.*

(B) *If $\gcd(a,p)=1$ and $b \equiv 0 \equiv x_0 \bmod p$, then $L_G(x_0;a,b;p^k)=1$ except for the case $p=2=k$ and $b \equiv 2 \bmod 4$. For this exceptional case, $L_G(x_0;a,b;4)=2$.*

(C) *If $\gcd(ab(x_0^2-bx_0+a),p)=1$ and $b^2+4a \equiv 0 \bmod p$, then $L_G(x_0;a,b;p^k)=p-1$.*

(D) *If p is odd, $\gcd(ab(b^2+4a),p)=1$, $x_0 \equiv b/2 \bmod p$, and the order $\mathfrak{o}(m_f)$ of the polynomial $m_f(x)=x^2+(b^2/a+2)x+1$ in $\mathrm{GF}(p)[x]$ is even, then $L_G(x_0;a,b;p^k)=\mathfrak{o}(m_f)-1$.*

(E) *If $\gcd(ab(b^2+4a)(x_0^2-bx_0+a),p)=1$, $x_0 \not\equiv b/2 \bmod p$ for $p \neq 2$, and the order $\mathfrak{o}(M_f)$ of the polynomial $M_f(x)=x^2-(2+(b^2+a)/(x_0^2-bx_0+a))x+1$ in $\mathrm{GF}(p)[x]$ divides $\mathfrak{o}(m_f)$, then $L_G(x_0;a,b;p^k)=\mathfrak{o}(m_f)-1$ except for the case $p=2=k$ and $a \equiv 1 \bmod 4$. For this exceptional case, $L_G(x_0;a,b;4)=4$.*

Proof. (A) From Lemma 1(A), $L_G(x_0;a,b;p)=1$. Since the sequence $X(x_0;a,b)$ with modulus p contains 0, $\gcd(b,p)=1$ implies $x_0 \equiv 0 \bmod p$ and so, $x_1 \equiv b \bmod p^k$ by Lemma 10 and the fact that $ax_0 \equiv 0 \bmod 4$ when $p=2$. In this case, it suffices to consider $X(b;a,b)$ with modulus p^k. Since $\gcd(b,p)=1$, $L_G(b;a,b;p^k)=1$ by Theorem 5(A) and so $L_G(x_0;a,b;p^k)=1$. Now, suppose $b \equiv 0 \bmod p$. From Lemma 1(A) again, $x_n \equiv b \equiv 0 \bmod p$. Then this case follows from Lemma 10 except for the case $p^k=4$. For this exception, $ab^{2-1}+b \equiv b \bmod 4$ since $\phi(4)=2$ and $a \equiv 0 \equiv b \bmod 2$. So, $x_n \equiv b \bmod 4$ for all $n \geq 1$. Therefore, $L_G(x_0;a,b;4)=1$.

From now on, let $\gcd(a,p)=1$. Then $X(x_0;a,b)$ with modulus p^k is purely periodic.

(B) From Lemma 1(B), $L_G(x_0;a,b;p)=1$. Then the case follows from Lemma 10 except for $p^k=4$. If $b \equiv 2 \bmod 4$, then $x_n \equiv 0 \bmod 2$ and $x_n \not\equiv x_{n+1} \bmod 4$ for all $n \geq 0$, because of $x_0 \equiv 0 \bmod 2$ and $\gcd(a,2)=1$. So, $L_G(x_0;a,b;4)=2$ if $b \equiv 2 \bmod 4$. If $b \equiv 0 \bmod 4$, then $x_n \equiv x_0 \bmod 4$ for all $n \geq 0$. Hence, $L_G(x_0;a,b;4)=1$ if $b \equiv 0 \bmod 4$.

(C) Note that $p \neq 2$ in this case. From Lemma 1(E)(2), the sequence $X(x_0; a, b)$ with modulus p contains 0 and so $L_G(x_0; a, b; p) = p - 1$. Then this case follows from Lemma 10.

(D) This case follows from Lemma 1(F)(2) and Lemma 10 immediately.

(E) This case follows from Lemma 1(F)(4) and Lemma 10 except for the case $p = 2 = k$. We now consider the exceptional case. Since $\gcd(ab, 2) = 1$, we have $a \equiv 1 \equiv b \bmod 2$. So, $a \equiv 1, 3 \bmod 4$, $b \equiv 1, 3 \bmod 4$, and $x_0 \equiv 0, 1, 2, 3 \bmod 4$. By checking all possible cases, $L_G(x_0; a, b; 4) = 2$ if $a \equiv 3 \bmod 4$, and $L_G(x_0; a, b; 4) = 4$ if $a \equiv 1 \bmod 4$. Finally, note that $m_f(x) = x^2 + x + 1$ in $\mathrm{GF}(2)[x]$ has order 3. This completes the proof of this theorem.

Let m, a, b and x_0 be integers with $m > 0$. Let the sequence $X(x_0; a, b)$ with modulus m be defined by the recursion (3). Huber [9] showed that if m is square free, then $X(x_0; a, b)$ with modulus m has the maximal period length if and only if the polynomial $f(x) = x^2 - bx - a$ is an IMP (abbreviated for inversive maximal period) polynomial in $\mathrm{GF}(p)[x]$ for every prime divisor p of m. So, if m is square free and $X(x_0; a, b)$ with modulus m has the maximal period length, then its period length is m. This is no more true if m is not square free. In fact, if $m = p_1 \ldots p_{s-1} p_s^{r_s} \ldots p_t^{r_t}$ is the prime factorization of m, where $p_1, \ldots, p_t$ are distinct primes and $r_s, \ldots, r_t$ are positive integers greater than 1, then the sequence $X(x_0; a, b)$ with modulus m has the maximal period length if and only if $f(x) = x^2 - bx - a$ is an IMP polynomial in $\mathrm{GF}(p_i)[x]$ for all $1 \leq i < s$, and a, b, x_0 and $p_j^{r_j}$ satisfy the conditions of Corollary 9 for all $s \leq j \leq t$.

Acknowledgements. The author is sincerely grateful to Prof. Dr. H. Niederreiter of the Institute of Information Processing, Austrian Academy of Sciences, Austria, for many helpful discussions and useful comments.

References

[1] W.-S. Chou, *On inversive maximal period polynomials over finite fields*, Appl. Algebra Engrg. Comm. Comput. 6 (1995), 245–250.

[2] —, *The period lengths of inversive pseudorandom vector generators*, Finite Fields Appl. 1 (1995), 126–132.

[3] J. Eichenauer and J. Lehn, *A non-linear congruential pseudorandom number generator*, Statist. Hefte 27 (1986), 315–326.

[4] J. Eichenauer, J. Lehn and A. Topuzoğlu, *A nonlinear congruential pseudorandom number generator with power of two modulus*, Math. Comp. 51 (1988), 757–759.

[5] J. Eichenauer-Herrmann, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. 60 (1992), 167–176.

[6] —, *Construction of inversive congruential pseudorandom number generators with maximal period length*, J. Comput. Appl. Math. 40 (1992), 345–349.

[7] J. Eichenauer-Herrmann and A. Topuzoğlu, *On the period length of congruential pseudorandom number sequences generated by inversions*, ibid. 31 (1990), 87–96.
[8] M. Flahive and H. Niederreiter, *On inversive congruential generators for pseudorandom numbers*, in: Finite Fields, Coding Theory, and Advances in Communications and Computing, G. L. Mullen and P. J.-S. Shiue (eds.), Marcel Dekker, New York, 1992, 75–80.
[9] K. Huber, *On the period length of generalized inversive pseudorandom generators*, Appl. Algebra Engrg. Comm. Comput. 5 (1994), 255–260.
[10] H. Niederreiter, *Finite fields and their applications*, in: Contributions to General Algebra, Vol. 7, Vienna, 1990, Teubner, Stuttgart, 1991.
[11] —, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, PA, 1992.
[12] —, *Pseudorandom vector generation by the inversive method*, ACM Trans. Modeling & Computer Simulation 4 (1994), 191–212.

INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
NANKANG, TAIPEI 11529
TAIWAN, ROC
E-mail: MACWS@CCVAX.SINICA.EDU.TW

Received on 13.4.1994
and in revised form on 15.9.1994 (2593)