On the multiplicative group generated by shifted binary quadratic forms

J.M. De Koninck and I. Kátai

Édition du 14 octobre 2002

§1. Introduction

Let E be a set of positive integers. We say that E is a set of uniqueness modulo 1 if for each completely additive function $f : \mathbf{N} \to \mathbf{R}/\mathbf{Z}$ for which $f(e) \equiv 0 \pmod 1$ for every $e \in E$, we necessarily have that $f(n) \equiv 0 \pmod 1$ for each positive integer n. Here and in what follows, we let $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{R}$ stand for the set of positive integers, all integers, rational numbers and real numbers, respectively; also p always stands for a prime number. It is clear that the domain of a completely additive function f can be extended to the multiplicative group of positive rationals, simply by setting

$$f(m/n) = f(m) - f(n) \quad \text{for each } m, n \in \mathbf{N}.$$

Let $\mathbf{Q}^*$ be the group of positive rationals, and for each positive integer h, let

$$Q_h^* := \{\frac{m}{n} : m, n \in \mathbf{N},\ (mn, h) = 1\}.$$

Let E^* be the multiplicative group generated by E. It was proved independently by several authors that E is a set of uniqueness mod 1 if and only if $E^* = \mathbf{Q}^*$; see for instance Indlekofer [5], Hoffman [3], Elliott [4] and Meyer [9]. It is not known whether the set of shifted primes is a set of uniqueness mod 1.

In Kátai [7], it was proved implicitly that the set of "primes + one" enlarged by a suitable finite set of primes is a set of uniqueness mod 1. Elliott [2] proved that the set of primes up to 10^{387} together with the set of shifted primes forms a set of uniqueness mod 1.

Let D be equal to 4 or 8 or an odd prime. Let $\chi_D = (\frac{-D}{n})$ be the Kronecker character and $\mathcal{B}(D)$ be the multiplicative semigroup generated by the union of the following four sets:

$$\{p : p|D\}, \qquad \{r^2 : r = 1, 2, 3, \ldots\}, \qquad \{p : \chi_{-D}(p) = 1\}, \qquad \{0\}.$$

From here on, we fix D and write χ instead of χ_D. Now let

$$w(n) := \sum_{d|n} \chi(d) = \prod_{p^\alpha \| n} \left(1 + \chi(p) + \ldots + \chi(p^\alpha)\right). \tag{2.1}$$

It is clear that an integer n coprime to D belongs to $\mathcal{B}(D)$ if and only if $w(n) > 0$. Furthermore, if $(n, D) = 1$, then it is well known that the number of representations of n by classes of binary quadratic forms with discriminant $-D$ is $\alpha w(n)$, where

$$\alpha = \begin{cases} 2 & \text{if } D > 4, \\ 4 & \text{if } D = 4, \\ 6 & \text{if } D = 3 \end{cases}$$

(see Landau [8]). Assume that A is a positive integer and set

$$E(D,A) := \{n+A : n \in \mathcal{B}(D)\}.$$

Let furthermore $\mathcal{H}(D,A)$ be the multiplicative group generated by $E(D,A)$.

In this paper, we give necessary and sufficient conditions under which $\mathcal{H}(D,A) = \mathbf{Q}^*$, at least in the case where D is a prime number.

Remarks.

(a) Fehér, Indlekofer and Timofeev [6] investigated the case $D = 4$ and proved that $\mathcal{H}(4,A) = \mathbf{Q}^*$, if A is the sum of two sqaures.

(b) Indlekofer claimed that he and Timofeev can prove that for every $k \in \mathbf{Q}^*$, there exist $n_1, n_2 \in \mathcal{B}(4)$ such that $n_1 + A = k(n_2 + A)$ provided $A > 0$.

(c) If $h(-D) = 1$, then $D = 4, 8$ or an odd prime, and $\mathcal{B}(D)$ can be interpreted as the set of those integers which can be written as the values of a binary quadratic form of discriminant $-D$.

§2. Main results

Theorem 1. *Let $D > 3$ be an arbitrary prime and let A be any given positive integer. Then*

$$\mathcal{H}(D,A) = \begin{cases} \mathbf{Q}_D^* & \text{if } \chi_D(A) = -1, \\ \mathbf{Q}^* & \text{otherwise.} \end{cases}$$

Theorem 2. *Let $D = 4$ and let A be an arbitrary positive integer. Then $\mathcal{H}(4,A) = \mathbf{Q}^*$.*

Theorem 3. *Let $D = 8$ and let A be an arbitrary positive integer. Then $\mathcal{H}(8,A) = \mathbf{Q}^*$.*

§3. Preliminary lemmas

Lemma 0. *Let χ be the Kronecker character mod $-D$, where $D > 0$. Let $U > 0$ and $V \neq 0$ be two integers for which there is an arithmetic progression $\ell \pmod D$ such that $\chi(\ell) = 1$ and such that $t := U\ell + V$ satisfies $\chi(t) = 1$. Moreover, let*

$$a(x) := \sum_{\substack{x<p\le 2x \\ p\equiv \ell \pmod D}} w(Up+V),$$

*where w is defined by (**??**). Then $a(x)$ is positive if x is sufficiently large.*

This result can easily be obtained by using the Bombieri-Vinogradov mean value theorem in the form

$$\sum_{k\le\sqrt{x}/(\log x)^{B+25}} \max_{\ell} \max_{n\le x} \left| \pi(u,k,\ell) - \frac{\mathrm{li}(x)}{\phi(k)} \right| \ll \frac{x}{\log^B x},$$

where li(x) stands for the logarithmic integral, and the "enveloping sieve" given by Hooley (see [4], Chapter 5), which Hooley used to obtain an asymptotic estimate for the number of solutions of the equation $n = p + x^2 + y^2$.

In the following lemmas, we assume that D is an odd prime and $(A, D) = 1$.

Lemma 1. *Let $k \equiv 1 \pmod D$ and $(k, A) = 1$. Then $k \in \mathcal{H}(D, A)$.*

Lemma 2. *Let $k \equiv \ell \pmod D$ and $(k\ell, AD) = 1$. Then $k/\ell \in \mathcal{H}(D, A)$.*

Lemma 3. *Let $\mathbf{Z}_D^*$ be the set of reduced residue classes mod D generated by*

$$\{\nu + A : \nu = 0 \text{ or } \nu = \text{ quadratic residue mod } D\ \} \setminus \{0\}, \tag{3.1}$$

and let $\mathcal{T}$ be a subgroup of $\mathbf{Z}_D^*$. Then $\mathcal{T} = \mathbf{Z}_D^*$.

Lemma 4. *Let $\chi(-A) = -1$. Then $\mathcal{H}(D, A) \subseteq \mathbf{Q}_D$.*

Lemma 5. *Let S_A be the multiplicative group generated by $E_1 \cup E_2$, where*

$$\begin{aligned} E_1 &= \{p + A : \chi(p) = 1,\ p \not\equiv -A \pmod{D}\}, \\ E_2 &= \{D^r + A : r = 1, 2, 3, \ldots\}. \end{aligned}$$

Then, for every $\nu \in \mathbf{Z}_D^*$, S_A contains infinitely many integers congruent to $\nu \pmod D$, all of which are coprime to A. Moreover, $S_A \subseteq \mathcal{H}(D, A)$.

Proof of Lemma 1. In order to prove that $k \in \mathcal{H}(D, A)$, it is sufficient to find $n_1, n_2 \in \mathcal{B}(D)$ such that $n_1 + A = k(n_2 + A)$. Let p run over the set of primes $p \equiv 1 \pmod D$ (so that $p \in \mathcal{B}(D)$) and consider the sum

$$a(x) := \sum_{x < p \le 2x} w(kp + (k-1)A).$$

It is enough to prove that $a(x)$ is positive for some x.

For this, we let $\ell(p) := kp + (k-1)A$ and observe that $\ell(p) \equiv 1 \pmod D$, so that $\chi(\frac{\ell(p)}{d}) = \chi(d)$. Consequently, using definition of w given in (**??**), we have

$$w(\ell(p)) = 2 \sum_{\substack{d \mid \ell(p) \\ d < \sqrt{\ell(p)}}} \chi(d) + E_p,$$

where $E_p = 0$ except when $\ell(p)$ is a square, in which case we get that $E_p = \chi\left(\sqrt{\ell(p)}\right)$, that is $|E_p| \le 1$.

Thus, given a large number B,

$$\begin{aligned} a(x) &= \sum_{d \le \sqrt{x}/\log^B x} 2\chi(d) \cdot \#\{p \in [x, 2x] : \ell(p) \equiv 0 \pmod{d}\} \\ &\quad + \sum_{\sqrt{x}/\log^B x < d \le \sqrt{2kx + (k-1)A}} 2\chi(d) \cdot \#\{p \in [x, 2x] : \ell(p) \equiv 0 \pmod{d},\ d^2 < \ell(p)\} + O(\sqrt{x}) \\ &= \Sigma_1 + \Sigma_2 + O(\sqrt{x}). \end{aligned}$$

Using the Bombieri-Vinogradov mean value theorem (stated above), one can obtain that

$$\Sigma_1 = 2\left(\mathrm{li}(2x) - \mathrm{li}(x)\right) \sum_{d \le \sqrt{x}/\log^B x} \frac{\chi(d)}{\phi(dD)} + O\left(\frac{x}{\log^{B_1} x}\right),$$

where B_1 can be taken arbitrarily large provided B is large enough.

The crucial step is the evaluation of Σ_2. This can be done by using Lemma 0. We shall not go into details, but one can easily deduce from this method that

$$a(x) = C(D)\frac{2x}{\log x} + o\left(\frac{x}{\log x}\right),$$

where $C(D) = \sum_{d=1}^{\infty} \frac{\chi(d)}{\phi(dD)}$, which proves Lemma 1.

Proof of Lemma 2. Since both $k\ell^{\phi(D)-2}$ and $\ell^{\phi(D)-1}$ are $\equiv 1 \pmod D$ and are coprime to A, and since they both belong to $\mathcal{H}(D,A)$, it follows that their ratio $k/\ell \in \mathcal{H}(D,A)$.

Proof of Lemma 3. Assume that $\mathcal{T}$ is a proper subgroup of $\mathbf{Z}_D^*$. Then $\#\mathcal{T} < D-1$, so that $\#\mathcal{T} \le (D-1)/2$. On the other hand, since the set of the generating elements contains $(D-1)/2$ members, then $\#\mathcal{T}$ must be eqal to $(D-1)/2$, so that $\mathcal{T}$ must be the subgroup of the quadratic residues mod D. This means that $\nu + A$ is a quadratic residue if ν is equal to zero or to a quadratic residue, except when $\nu = -A$. (Observe that, in the case $\chi(-A) = -1$, $\mathcal{T}$ always has at least $(D+1)/2$ elements, so that $\#\mathcal{T} = D-1$, in which case $\mathcal{T} = \mathbf{Z}_3^*$.) Thus

$$\sum_{m=0}^{D-1} (\chi(m)+1)(\chi(m+A)+1) \ge 2 + 4\cdot\frac{D-3}{2}. \tag{3.2}$$

But, since

$$\sum_{m=0}^{D-1} \chi(m) = \sum_{m=0}^{D-1} \chi(m+A) = 0 \quad \text{and} \quad \sum_{m=0}^{D-1} \chi(m)\chi(m+A) = -1,$$

it follows that the left hand side of (3.2) is $D-1$ and therefore that $D - 1 \ge 2 + 4\cdot\frac{D-3}{2}$, which is impossible if $D > 3$.

So let $D = 3$. If $A \equiv 1 \pmod 3$, then the set $\{0+1 \pmod 3, 1+1 \pmod 3\}$ generates $\mathbf{Z}_3^*$. If $A \equiv -1 \pmod 3$, then $(-1) \pmod 3 \in \mathcal{T}$ and $(-1)^2 \pmod 3 \in \mathcal{T}$, so that $\mathcal{T} = \mathbf{Z}_3^*$.

Proof of Lemma 4. It is enough to show that $(n+A, D) = 1$ for every $n \in \mathcal{B}(D)$. Indeed, if $n + A \equiv 0 \pmod D$, then $\chi(n) \equiv \chi(-A) = 1$ and consequently $(n, D) = 1$. But $n \in \mathcal{B}(D)$ and $(n, D) = 1$ imply that $\chi(n) = 1$.

Proof of Lemma 5. These results are direct consequences of Lemma 3.

§4. Proof of Theorem 1

Assume first that $(A, D) = 1$. Then it follows from Lemmas 1,2,3,4,5 that

$$\mathbf{Q}^*_{AD} \subseteq \mathcal{H}(A, D).$$

Let $A = \pi_1^{\alpha_1}\pi_2^{\alpha_2}\dots\pi_r^{\alpha_r}$. We shall prove that $\pi_j \in \mathcal{H}(A, D)$ for $j = 1, 2, \dots, r$, which will imply that

$$\mathbf{Q}^*_D \subseteq \mathcal{H}(A, D). \tag{4.1}$$

So let π_1 be one of the prime divisors of A and write $A = \pi_1^{\alpha_1}A_2$.

Assume first that $\alpha_1 = 1$. Then for $m \in \mathcal{B}(D)$, we have

$$\mathcal{H}(A, D) \ni \pi_1^2 Dm + A = \pi_1 (\pi_1 Dm + A_2).$$

Since $(\pi_1 Dm + A_2, AD) = 1$, it follows that $\pi_1 Dm + A_2 \in \mathcal{H}(A, D)$, and so $\pi_1 \in \mathcal{H}(A, D)$.

For $\alpha_1 > 1$, we consider separately the cases α_1 odd and α_1 even.

First assume that $\alpha_1 = 2\beta + 1$, with $\beta \geq 1$. Then we have

$$\pi_1^{2\beta+2}Dm + \pi_1^{2\beta+1}A_2 = \pi_1^{2\beta+1}(\pi_1 Dm + A_2) \in \mathcal{H}(A, D).$$

Since $(\pi_1 Dm + A_2, AD) = 1$, we obtain that $\pi_1 Dm + A_2 \in \mathcal{H}(A, D)$ and consequently that $\pi_1^{2\beta+1} \in \mathcal{H}(A, D)$. Furthermore, if $m \in \mathcal{B}(D)$, then $\pi_1^2 Dm + A \in \mathcal{H}(A, D)$ and $\pi_1^2 Dm + A = \pi_1^2(Dm + \pi_1^{2\beta-1}A_2)$, whence $\pi_1^2 \in \mathcal{H}(A, D)$ follows by observing that $(Dm + \pi_1^{2\beta-1}A_2, AD) = 1$. Thus

$$\pi_1 = \frac{\pi_1^{2\beta+1}}{(\pi_1^2)^\beta} \in \mathcal{H}(A, D).$$

Let us now consider the case $\alpha = 2\beta$ with $\beta \geq 1$. Starting from $m \in \mathcal{B}(D)$,

$$\mathcal{H}(A, D) \ni \pi_1^{2\beta+2}Dm + A = \pi_1^{2\beta}\left(D\pi_1^2 m + A_2\right),$$

$(D\pi_1^2 m + A_2, AD) = 1$, it follows that $D\pi_1^2 m + A_2 \in \mathcal{B}(D)$, and therefore that $\pi_1^{2\beta} \in \mathcal{B}(D)$.

We shall now prove that $\pi_1^2 \in \mathcal{H}(A, D)$. Since we already proved this in the case $\beta = 1$, we may assume that $\beta \geq 2$ and consider the integer $\pi_1^2 D + A = \pi_1^2\left(D + \pi_1^{2(\beta-1)}A_2\right)$. Since $\pi_1^2 D + A \in \mathcal{H}(A, D)$, $D + \pi_1^{2(\beta-1)}A_2 \in \mathcal{H}(A, D)$, we obtain that $\pi_1^2 \in \mathcal{H}(A, D)$, as claimed.

Finally, we observe that tehre is some $m \in \mathcal{B}(D)$ such that $\pi_1 \| mD + A_2$. This is true if $Dm + A_2 \equiv \pi_1 \pmod{\pi_1^2}$, which defines an arithmetic progression $m \equiv s \pmod{\pi_1^2}$, where $S = (\pi_1 - A_2)D^{-1} \pmod{\pi_1^2}$, $(s, \pi_1) = 1$. If m is a prime p satisfying $p \equiv s \pmod{\pi_1^2}$, $p \equiv 1 \pmod{D}$, then it is a suitable choice for $m \in \mathcal{B}(D)$, $\pi_1 \| Dm + A_2$.

Hence $Dm + A_2 = \pi_1\eta$ with $(\eta, DA) = 1$ and $\eta \in \mathcal{H}(A, D)$; furthermore, $\pi_1^{2\beta}Dm + A = \pi_1^{2\beta}(Dm + A_2)$. Thus $\pi_1 \in \mathcal{H}(A, D)$ and since π_1 was an arbitrary prime divisor of A, our claim (4.1) is established.

Let us now investigate whether D belongs to $\mathcal{H}(A, D)$ or not. Since we already proved that it cannot hold if $\chi(-A) = -1$, we may assume that $\chi(-A) = 1$. Then $p \equiv -A$

(mod D) implies that $p+A \in \mathcal{H}(A,D)$. There are infinitely many primes p such that $D \| p+A$, that is $\frac{p+A}{D} = \eta_p$ with $(\eta_p, D) = 1$ and $\eta_p \in \mathcal{H}(A,D)$, and consequently $D \in \mathcal{H}(A,D)$. Thus the theorem is proved in the case $(A,D) = 1$. Hence we shall now assume that $A = D^r B$ with $(B,D) = 1$ and $r \geq 1$. We shall try to find integers $n_1, n_2 \in \mathcal{B}(D)$ such that $n_1 + A = D(n_2 + A)$, that is $n_1 - Dn_2 = (D-1)A$. We shall find these by looking for m_1, m_2's such that $n_1 = D^r m_1$, $n_2 = D^r m_2$, which leads to the equation

$$m_1 - m_2 = (D-1)B. \tag{4.2}$$

Let ν run over zero and the quadratic residues mod D, that is over $\frac{D+1}{2}$ integers, and let $(H,D) = 1$. Then the set $\{\nu + H\}$ contains either a quadratic residue or zero. This is true in particular if we choose $H = (D-1)B$. So let ν, μ be such a couple of residues for which

$$\nu - \mu = (D-1)B, \qquad \chi(\nu) \neq -1, \qquad \chi(\mu) \neq -1.$$

If $\mu \not\equiv 0 \pmod{D}$, consider the sum

$$\sum_{\substack{x<p\leq 2x \\ p\equiv\mu \pmod{D}}} w(p + (D-1)B). \tag{4.3}$$

If $\mu \equiv 0 \pmod{D}$, then consider the sum

$$\sum_{\substack{x<p\leq 2x \\ p\equiv 1 \pmod{D}}} w(Dp + (D-1)B). \tag{4.4}$$

By using the Bombieri-Vinogradov mean value theorem and the evaluating sieve of Hooley mentioned above, one can deduce that both expressions (4.3) and (4.4) are positive provided x is large enough, in which case there exists at least one pair of integers $n_1, n_2 \in \mathcal{B}(D)$ for which

$$D = \frac{n_1 + A}{n_2 + A}.$$

The proof of Theorem 1 is thus complete.

§5. Proof of Theorem 2

Assume first that A is odd. We shall prove that

$$k = \frac{n_1 + A}{n_2 + A}, \qquad n_1, n_2 \in \mathcal{B}(4) \tag{5.1}$$

can be solved if $k \equiv 1 \pmod{4}$, $(k,A) = 1$. Let n_2 run over the primes $p \equiv 1 \pmod{4}$ and $n_1 = kp + (k-1)A$. By using the method of §4, one can prove that

$$\sum_{\substack{p<x \\ p\equiv 1 \pmod{4}}} w(kp + (k-1)A) > 0$$

provided x is large enough, in which case (5.1) has a solution.

Hence we can deduce that for $k \equiv \ell \equiv 3 \pmod 4$, $(k\ell, A) = 1$, we have

$$k/\ell \in \mathcal{H}(4, A), \tag{5.2}$$

simply by repeating the argument used in the proof of Lemma 2.

Since $A+4, A+2 \in \mathcal{H}(4, A)$, there exists at least one $\nu \in \mathcal{H}(4, A)$ for which $\nu \equiv 3 \pmod 4$ and $(\nu, A) = 1$. Hence we obtain as earlier that

$$\mathbf{Q}_{4A}^* \subseteq \mathcal{H}(4, A).$$

Let $A = \pi_1^{\alpha_1} A_2$, $(A_2, \pi_1) = 1$, π_1 prime. We shall prove that $\pi_1 \in \mathcal{H}(4, A)$. Since π_1 is an arbitrary prime divisor of A, it will be true for each prime divisor of A, which implies that

$$\mathbf{Q}_4 \subseteq \mathcal{H}(4, A). \tag{5.3}$$

Assume first that $\alpha_1 = 1$. Then $4\pi_1^2 + A_2\pi_1 = \pi_1(4\pi_1 + A_2)$ with $(4\pi_1 + A_2, 4A) = 1$, whence $\pi_1 \in \mathcal{H}(4, A)$.

Now consider the case $\alpha_1 = 2\beta + 1$, $\beta \geq 1$. By setting $4\pi_1^2 + A_2\pi_1^{2\beta+1} = \pi_1^2(4 + A_2\pi_1^{2\beta-1})$, we obtain that $\pi_1^2 \in \mathcal{H}(4, A)$. Then by considering $4\pi_1^{2\beta+2} + \pi_1^{2\beta+1}A_2 = \pi_1^{2\beta+1}(4\pi_1 + A_2)$ and observing that $4\pi_1 + A_2 \in \mathcal{H}(4, A)$, it follows that $\pi_1^{2\beta+1} \in \mathcal{H}(4, A)$, and hence that $\pi_1 \in \mathcal{H}(4, A)$.

Finally, let $\alpha = 2\beta$, $\beta \geq 1$. Similarly, by choosing the numbers $4\pi_1^{2\beta+2} + A$ and $4\pi_1^2 + A$, we first deduce that $\pi_1^2 \in \mathcal{H}(4, A)$.

Arguing as in the proof of Theorem 1, we first prove that there is at least one (actually infinitely many) $m \in \mathcal{B}(4)$ such that $Dm + A_2 \equiv \pi_1 \pmod{\pi_1^2}$. If such an integer m exists, then the integer $\eta_m = \frac{Dm+A_2}{\pi_1}$ is coprime to AD. Consequently $\eta_m \in \mathcal{H}(4, A)$ and furthermore $\pi_1^{2\beta+1}\eta_m = Dm\pi_1^{2\beta} + A \in \mathcal{H}(4, A)$, whence $\pi_1^{2\beta+1} \in \mathcal{H}(4, A)$, and so $\pi_1 \in \mathcal{H}(4, A)$.

It remains to prove the existence of such an integer m. To do so, it is enough to observe that there is at least one (actually infinitely many) prime $p \equiv 1 \pmod 4$ such that $4p + A_2 \equiv \pi_1 \pmod{\pi_1^2}$. Since this clearly holds, we have thus established (5.3).

We shall now prove that $2 \in \mathcal{H}(4, A)$.

If $A \equiv 1 \pmod 4$, then $2 \| 1 + A$ and $1 + A \in \mathcal{H}(4, A)$ imply that $2 \in \mathcal{H}(4, A)$.

If $A \equiv 3 \pmod 4$, then $A = -1 + 2^\gamma B$, with B odd and $\gamma \geq 2$. For every $\varepsilon > \gamma$, the number of primes $p < x$ for which $2^\varepsilon \| p + A$ is $(1 + o(1))\mathrm{li}(x)/2^{\varepsilon-1}$, which means that there exists a prime p_ε and an odd integer η_ε such that $p_\varepsilon + A = 2^\varepsilon \eta_\varepsilon$ with $\eta_\varepsilon \in \mathcal{H}(4, A)$. It is obvious that $p_\varepsilon \equiv 1 \pmod 4$ and thus that $p_\varepsilon + A \in \mathcal{H}(4, A)$. Hence

$$2 = \frac{2^{\varepsilon+1}}{2^\varepsilon} = \frac{p_{\varepsilon+1} + 1}{\eta_{\varepsilon+1}} \cdot \frac{\eta_\varepsilon}{p_\varepsilon + 1} \in \mathcal{H}(4, A).$$

We have thus proved that $\mathcal{H}(4, A) = \mathbf{Q}^*$ if $(A, 2) = 1$.

Assume now that $A = 2^\gamma B$ with B odd and $\gamma \geq 1$. We already proved that $\mathcal{H}(4, B) = \mathbf{Q}^*$, that is that each rational number m/n has a representation

$$\frac{m}{n} = \prod_{j=1}^{r} (n_j + B)^{\varepsilon_j},$$

where $\varepsilon_j \in \{-1, 1\}$ and $n_j \in \mathcal{B}(4)$, and so

$$\frac{m}{n} = 2^{\gamma(\varepsilon_1 + \ldots + \varepsilon_r)} \prod_{j=1}^{r} (2n_j + A)^{\varepsilon_j}.$$

To complete the proof of Theorem 2, it is enough to show that $2 \in \mathcal{H}(4, A)$. But this is true if

$$n_1 + A = 2(n_2 + A), \qquad n_1, n_2 \in \mathcal{B}(4)$$

can be solved. By writing $n_1 = 2^\gamma m_1$, $n_2 = 2^\gamma m_2$, it follows that the existence of $m_1, m_2 \in \mathcal{B}(4)$, with $m_1 - 2m_2 = B$, would be enough.

Now if $B \equiv 1 \pmod 4$, then let m_2 run over the set $\{2p : p \equiv 1 \pmod 4\}$ and consider the sum

$$\sum_{\substack{p \le x \\ p \equiv 1 \pmod 4}} w(4p + B),$$

which is surely positive if x is large enough.

On the other hand, if $B \equiv -1 \pmod 4$, then let m_1 run over the set $\{2p : p \equiv 1 \pmod 4\}$ and consider the slightly diffrent sum

$$\sum_{\substack{p \le x \\ p \equiv 1 \pmod 4}} w(2p + B),$$

which again is surely positive if x is large enough.

This completes the proof of Theorem 2.

§6. Proof of Theorem 3

Since the proof is very similar to that of Theorems 1 and 2, we shall only give a sketch of it.

Observe that now $D = 8$ and

$$\chi(1) = \chi(3) = 1, \quad \chi(5) = \chi(7) = -1.$$

Assume first that A is odd. By arguing as earlier, we can deduce that

$$\mathbf{Q}_{2A}^* \subseteq \mathcal{H}(8, A).$$

Repeating the argument used before, one can prove that $\pi \in \mathcal{H}(8, A)$ if π is a prime divisor of A. Consequently,

$$\mathbf{Q}_2^* \subseteq \mathcal{H}(8, A).$$

Since $A+1, A+3 \in \mathcal{H}(8, A)$ and since either $2 \| A+1$ or $2 \| A+3$, we obtain that $2 \in \mathcal{H}(8, A)$, and so

$$\mathbf{Q}_4^* \subseteq \mathcal{H}(8, A).$$

The theorem is thus proved for A odd. So let $A = 2^\gamma B$ with B odd and $\gamma \geq 1$. As earlier, we can deduce that each rational number m/n can be written as

$$\frac{m}{n} = 2^{\Gamma(m,n)}\alpha(m,n),$$

where $\Gamma(m,n)$ is a positive integer depending on m and n, and $\alpha(m,n) \in \mathcal{H}(8,A)$.

Thus it remains to prove that $2 \in \mathcal{H}(8,A)$. For this we try to solve the equation $n_1 + A = 2(n_2 + A)$, that is $n_1 - 2n_2 = A$. So let $n_1 = 2^\gamma m_1$, $n_2 = 2^\gamma m_2$, that is $m_1 - 2m_2 = B$. Let us now choose m_1 as follows

$$m_1 = \begin{cases} 2p + B & \text{with } p \equiv 1 \pmod 8 \text{ if } B \equiv 1 \pmod 8, \\ 2p + B & \text{with } p \equiv 3 \pmod 8 \text{ if } B \equiv 5 \pmod 8, \\ 8p + B & \text{with } p \equiv 1 \pmod 8 \text{ if } B \equiv 3 \pmod 8, \\ 2p + B & \text{with } p \equiv 1 \pmod 8 \text{ if } B \equiv 7 \pmod 8. \end{cases}$$

Since each of the above choices has at least one solution $m_1 \in \mathcal{B}(8)$, this completes the proof of Theorem 3.

References

[1] P.D.T.A. Elliott, *Arithmetic Functions and Integer Products*, Springer-Verlag, 1985.

[2] P.D.T.A. Elliott, *On representing integers as products of the* $p+1$, Monatsh. Math. **97** (1984), no. 2, 85-97.

[3] P. Hoffmann, *Note on a problem of Kátai*, Acta Math. Hung, **45** (1985), 261-262.

[4] C. Hooley, *Application of Sieve Methods to the Theory of Nunbers*, Cambridge University Press, 1976.

[5] K.-H. Indlekofer, *On sets characterixing additive and multiplicative functions*, Ill. J. Math. **25** (1981), 251-257.

[6] J. Fehér, K.-H. Indlekofer and N.M. Timofeev, *A set of uniqueness for completely additive arithmetic functions*, Annales Univ. Sci. Budapest, Sect. Comp. **21** (2002), 57-67.

[7] I. Kátai, *On sets characterizing number theoretical functions II. The set of "primes plus one" is a set of uniqueness*, Acta Arith. **16** (1969/1970, 1-4.

[8] E. Landau, *Vorlesungen über Zahlentheorie. I-III.* S. Hirzel, Leipzig. English translation of Vol. I: Chelsea, New York, 1958.

[9] F. Meyer, *Ensemble d'unicité pour les fonctions additives. Étude analogue dans le cas des fonctions multiplicatives*, Journées de Théorie Analytique et Élémentaire des nombres, Orsay, 2 et 3 juin, 1980. Publications Mathématiques d'Orsay, 50-66.

Jean-Marie De Koninck
Département of mathématiques
Université Laval
Québec G1K 7P4
Canada

Imre Kátai
Computer Algebra Department
Eötvös Loránd University, H-1177
Budapest, Pázmány Péter Sétány I/C
Hungary

Lemma 1. *Let A and D be positive integers. If $k \in \mathbf{N}$ is coprime to D, $\ell \equiv k \pmod{D}$, then $k/\ell \in \mathcal{F}(D, A)$.*

Proof. First observe that it is enough to prove the result for a general k and corresponding $\ell = k + D$. Indeed, if $\frac{k}{k+D} \in \mathcal{F}(D, A)$, then for $\ell = k + hD$, we have that

$$\frac{k}{\ell} = \frac{k}{k+D} \cdot \frac{k+D}{k+2D} \cdot \ldots \cdot \frac{k+(h-1)D}{k+hD} \in \mathcal{F}(D, A).$$

Hence let k, ℓ be fixed, $l = k + D$, $(k, \ell) = 1$, and assume that X is large. Let us consider the sum

$$\Sigma_0 := \sum r(n_1) r(n_2),$$

where the summation runs over those $n_1, n_2 \in \mathcal{B}_d$ for which $n_1 \equiv 1 \pmod{D}$, $n_2 \in [X, 2X]$ and

$$k(n_1 + A) = \ell(n_2 + A) \tag{5.4}$$

holds. We shall prove that $\Sigma_0 > 0$ which will complete the proof of Lemma 1. In fact we shall prove more, namely that if X is sufficiently large, then $\Sigma_0 > cX$ with some positive constant c.

Observe that, if (5.4) holds, then $n_2 \equiv 1 \pmod{D}$, and also that

$$r(n_1) = \sum_{\substack{\delta_1 | n_1 \\ \delta_1 < \sqrt{n_1}}} \chi(\delta_1), \qquad r(n_2) = \sum_{\substack{\delta_2 | n_2 \\ \delta_2 < \sqrt{n_2}}} \chi(\delta_2),$$

assuming that n_1 and n_2 are not square numbers. Thus Σ_0 can be written as (neglecting some error term $O(\sqrt{x})$)

$$\sum_{\substack{\delta_1 < \sqrt{2X} \\ \delta_2 < \sqrt{\frac{k}{\ell}(2X+a) - A}}} \chi(\delta_1)\chi(\delta_2) N_X(\delta_1, \delta_2), \tag{5.5}$$

where $N_X(\delta_1, \delta_2)$ is the smallest of those integers u_1, u_2 for which

$$(k + D)\delta_2 u_2 - k\delta_1 u_1 = DA \tag{5.6}$$

and the following conditions hold:

$$\delta_1 u_1 \equiv 1 \pmod{D}, \quad \delta_1 u_1 \in [X, 2X], \quad \delta_1 < u_1, \quad \delta_2 < u_2.$$

If we sum the expression (5.5) only for those δ_1, δ_2 for which $\delta_1 < \dfrac{\sqrt{X}}{(\log X)^B}$ and $\delta_2 < \dfrac{\sqrt{X}}{(\log X)^B}$, then it can easily be shown, using sieve theorems, that the error we then introduce is $o(X)$.

Hence let δ_1, δ_2 be fixed, $e := \mathrm{GCD}((k + D)\delta_2, k\delta_1)$. If (5.6) has at least one solution, then $e|DA$, in which case $e|A$, since $(\delta_1\delta_2 k(k + D), D) = 1$. Therefore it follows that under the above conditions, the number of solutions of (5.6) is

$$\frac{Xe}{D\delta_1\delta_2(k + D)} + O(1)$$

which implies that

$$\Sigma_0 = \frac{X}{D(k+D)} \sum_{e|A} e \sum_{\substack{\delta_1,\delta_2<\sqrt{X}/(\log X)^B \\ ((k+D)\delta_2, k\delta_1)=e}} \frac{\chi(\delta_1)\chi(\delta_2)}{\delta_1\delta_2}.$$

$$\vdots$$

$$\vdots$$

Lemma 2. *Let $(\ell, D) = 1$, $\chi(\ell) = 1$. Then $\ell + A \in \mathcal{F}(D, A)$.*

Proof. In light of Lemma 1, it is enough to prove that there exits a positive integer $n \equiv \ell \pmod D$ for which $r(n) > 0$. In order to prove this, we first set

$$A(X) := \sum_{\substack{n\in[X,2X] \\ n\equiv \ell \pmod D}} r(n).$$

We then have

$$\begin{aligned} A(X) &= \sum_{\delta<\sqrt{X}/(\log X)^B} \chi(\delta) \sum_{\substack{n\in[X,2X] \\ \delta|n,\ n\equiv\ell \pmod D}} 1 + o(X) \\ &= \frac{X}{D} \sum_{\delta<\sqrt{X}/(\log X)^B} \frac{\chi(\delta)}{\delta} + o(X) = \frac{X}{D} L(1,\chi_D) + o(X). \end{aligned}$$

Since we know that $L(1, \chi_D) > 0$, the proof of Lemma 2 is complete.

Lemma 3. *Let $D > 3$ be a prime number and let m be a positive integer not divisible by D. Then $m \in \mathcal{F}(D, A)$.*

Proof. Since $Q(0, 0) + A = A \in \mathcal{F}(D, A)$, it follows from Lemma 2 that $\nu + A \in \mathcal{F}(D, A)$ if $\nu = 0$, or $\nu \in [1, D-1]$, $\chi_D(\nu) = 1$. The set of these numbers is of size $\frac{D+1}{2}$, and at most one of of its members is 0 mod D.

Now let $\mathcal{T}$ be the subgroup of the set of all reduced residue classes modulo D which is generated by

$$\{\nu + A,\ \nu \neq -A,\ \nu = 0 \text{ or a quadratic residue}\}.$$

Then iether $\mathcal{T} = \mathbf{Z}_D^*$, in which case $\#\mathcal{T} = D-1$ or $\#\mathcal{T} \neq D-1$. In this last case, $\#\mathcal{T} \leq \frac{D-1}{2}$. If $\#\mathcal{T} = \frac{D-1}{2}$, then $\mathcal{T}$ is the group of all the quadratic residues, in which case the residue classes listed above must coincide with the quadratic residues, which implies that

$$\sum_{m=0}^{D-1} (\chi(m)+1)(\chi(m+A)+1) \geq 2 + 4\frac{D-3}{2}. \tag{5.7}$$

But $0 = \sum_{m=0}^{D-1} \chi(m) = \sum_{m=0}^{D-1} \chi(m+A)$, while $\sum_{m=0}^{D-1} \chi(m)\chi(m+A) = -1$, which means that the left hand side of (5.7) is $D - A$, so that $D - A \geq 2 + 2(D-3)$, which cannot hold if $D > 3$, thus completing the proof of Lemma 3.

Lemma 4. *Let $D = 3$. If $A \equiv 1 \pmod 3$, then*

$$\mathcal{F}(D, A) = \mathbf{Q}_3^*. \tag{5.8}$$

If $A \not\equiv 1 \pmod 3$, then $\mathcal{F}(D, A) = \mathbf{Q}^*$.

Proof. Under the stated conditions, the class number is 1, and the corresponding binary quadratic form can be written as

$$Q(x, y) = x^2 + xy + y^2.$$

Assume first that $A \equiv 1 \pmod 3$. Observe tht $Q(x, y)$ cannot take on values from the arithmetic progression $2 \pmod 3$, that is $Q(x, y) + A$ is not a multiple of 3 for any $x, y \in \mathbf{N}_0$. Thus $\mathcal{F}(3, D) \subset \mathbf{Q}_3^*$. But $Q(1, 0) + A = A + 1 \in \mathcal{F}(3, A)$; thus, since $A + 1 \equiv 2 \pmod 3$, (5.8) follows from Lemma 3.

If $A \equiv 2 \pmod 3$, then from $Q(0, 0) + A \in \mathcal{F}(3, A)$, and so by Lemma 2, we have that $\frac{m}{n} \in \mathcal{F}(3, A)$ provided $(mn, 3) = 1$. Now let t be a positive integer satisfying

$$3 \| Q(2^t, 0) + A = 2^{2t} + A.$$

Since $2^{2t} + A \in \mathcal{F}(3, A)$ and $(\frac{2^{2t}+A}{3}, 3) = 1$, it follows that $\frac{2^{2t}+A}{3} \in \mathcal{F}(3, A)$. Consequently, $3 \in \mathcal{F}(3, A)$.

It remains to consider the case when $A \equiv 0 \pmod 3$. So let $A = 3^\nu B$, $(B, 3) = 1$. If $\nu \geq 2$, then $Q(1, 1) + 3^\nu B = 3(1 + 3^{\nu-1}B) \in \mathcal{F}(3, A)$ and since $1 + 3^{\nu-1}B \in \mathcal{F}(3, A)$, we have that $3 \in \mathcal{F}(3, A)$ and so $\frac{A}{3^\nu} = B \in \mathcal{F}(3, A)$. Now if $B \equiv 2 \pmod 3$, then we have found an integer $\equiv 2 \pmod 3$ belonging to $\mathcal{F}(3, A)$; therefore all those numbers in the same arithmetic progression also belong to $\mathcal{F}(3, A)$, and we are done.

On the other hand, if $B \equiv 1 \pmod 3$, then we first observe that $3^\nu \in \mathcal{B}_3$, which implies that $3^\nu + 3^\nu B \in \mathcal{F}(3, A)$, whence $B + 1\ (\equiv 2 \pmod 3) \in \mathcal{F}(3, A)$, which clears this case as well.

Finally we consider the case $\nu = 1$, $A = 3B$. If $B \equiv 1 \pmod 3$, then $A, B \in \mathcal{F}(3, A)$ imply that $3 \in \mathcal{F}(3, A)$, and $3 \in \mathcal{B}_3$, $3 + 3B \in \mathcal{F}(3, A)$, and therefore $1 + B\ (\equiv 2 \pmod 3)$ belongs to $\mathcal{F}(3, A)$. We are left to consider the case $B \equiv 2 \pmod 3$. Since $A \in \mathcal{F}(3, A)$, it follows that B and $1/3$ are conjugates. So let $B = 2 + 3^\alpha z$, where $\alpha \geq 1$ and $(z, 3) = 1$. Since $21 \in \mathcal{B}_3$, $21 = 3A = 3^3(1 + 3^{\alpha-2}z)$ if $\alpha \geq 3$, we have that $21 + 3A \in \mathcal{F}(3, A)$, $1 + 3^{\alpha-2}z \in \mathcal{F}(3, A)$, thus implying that $3^3 \in \mathcal{F}(3, A)$. Since $A = 3B \in \mathcal{F}(3, A)$, we have that $A^2 = 9B^2 \in \mathcal{F}(3, A)$, and since $B^2 \equiv 1 \pmod 3$, then $3^2 \in \mathcal{F}(3, A)$, whence $3 = \frac{3^3}{3^2} \in \mathcal{F}(3, A)$, and so $\frac{A}{3} = B \in \mathcal{F}(3, A)$.

For the case $\alpha = 2$, we choose $12 \in \mathcal{B}_3$, so that $\mathcal{F}(3, A) \ni 3B + 12 = 3(4 + 2 + 9z) = 3^2(2 + 3z)$. Since $3^2 \in \mathcal{F}(3, A)$, we thus have that $2 + 3z \in \mathcal{F}(3, A)$.

The final case is $\alpha = 1$. Since there exists a prime $p \equiv 7 \pmod 9$ with $p \in \mathcal{F}(3, A)$ and $3p \in \mathcal{B}_3$, then writing $p = 7 + 9\lambda$, we have $\mathcal{F}(3, A) \ni 3p + A = 27\lambda + 21 + 6 + 9z = 9(3\lambda + 3 + z)$.

Assume first that $z \equiv 2 \pmod 3$. Since $9 \in \mathcal{F}(3,A)$, it follows that $3(\lambda+1)+z \in \mathcal{F}(3,A)$. But since this number is $\equiv 2 \pmod 3$, we are done. On the other hand, if $z \equiv 1 \pmod 3$, then simply observe that $\mathcal{F}(3,A) \ni 3+A = 9(1+z)$, and thus since $1+z \equiv 2 \pmod 3$ and $9 \in \mathcal{F}(3,A)$, we may conclude that $1+z \in \mathcal{F}(3,A)$.

The proof of Lemma 4 is thus complete.

§4. The proof of Theorem 1

The case $D=3$ was handled by Lemma 4. Hence we may assume that $D>3$. Now observe that Lemma 3 gives that $\mathcal{F}(D,A) \supseteq \mathbf{Q}_D^*$. We shall first assume that $D|A$. Then we clearly have that $A \in \mathcal{F}(D,A)$ since $0 \in \mathcal{B}_D$. If $d\|A$, $A = DB$, $(B,D)=1$, then $B \in \mathcal{F}(D,A)$, which implies that $D \in \mathcal{F}(D,A)$ and therefore that $\mathcal{F}(D,A) = \mathbf{Q}^*$. It is clear that $\mathcal{B}_D \ni D$, consequently $D\|D+A$ if $D^2|A$, whence $1+A/D \in \mathcal{F}(D,A)$, and since $D(1+A/D) \in \mathcal{F}(D,A)$, we conclude that $D \in \mathcal{F}(D,A)$, and therefore that $\mathcal{F}(D,A) = \mathbf{Q}^*$.

Assume now that $(A,D)=1$, and $\chi_D(-A)=-1$. Then $r(n)=0$ if $n \equiv -A \pmod D$. Consequently $(n+A,D)=1$ whenever $r(n)>0$. Thus in this case, $\mathcal{F}(D,A) = \mathbf{Q}_D^*$.

Assume finally that $\chi_D(-A)=1$, and let

$$\pi_j = -A + jD \pmod{D^2} \qquad (j = 0,1,\ldots,D-1).$$

Then each arithmetical progression $\pi_j \pmod{D^2}$ contains at least one prime p_j, $r_D(p_j)>0$, $p_j + A \in \mathcal{F}(D,A)$, and for some j, $D\|p_j+A$. Therefore $D \in \mathcal{F}(D,A)$ and $\mathcal{F}(D,A) = \mathbf{Q}^*$, thus completing the proof of Theorem 1.

§5. The proof of Theorem 2

Since $0,1,2,4$ belong to $\mathcal{B}_4$, there is an element in $\mathcal{F}(4,A)$ from the arithmetical progression $3 \pmod 4$ if $A \equiv -1$ or $1 \pmod 4$, that is if A is odd. In these cases, $\mathbf{Q}_2^* \subset \mathcal{F}(4,A)$. If $A = 1+4B$, then $A+1 = 2(1+2B) \in \mathcal{F}(4,A)$ and $1+2B \in \mathbf{Q}_2^* \subset \mathcal{F}(4,A)$. Therefore $2 \in \mathcal{F}(4,A)$ and thus $\mathcal{F}(4,A) = \mathbf{Q}^*$.

We are left to consider the case $A \equiv 3 \pmod 4$. For this let us write $A = -1+2^\gamma B$, $\gamma \geq 2$, B odd. We have $A+1 = 2^\gamma B$, $B \in \mathcal{F}(4,A)$, $A+1 \in \mathcal{F}(4,A)$, which implies that $2^\gamma \in \mathcal{F}(4,A)$. Now $5 \in \mathcal{F}(4,A)$ so that $5+A = 4(2^{\gamma-2}B+1)$. If $\gamma>2$, then $2^{\gamma-2}B+1 \in \mathcal{F}(4,A)$, and consequently $4 \in \mathcal{F}(4,A)$. If γ is odd, then $2^{\gamma-[\frac{\gamma}{2}]\cdot 2} = 2 \in \mathcal{F}(4,A)$. It remains to consider the case where γ is even, say $\gamma = 2\delta$. It is enough to prove that there is an odd exponent ε such that

$$2^\varepsilon \| \left(2^{2\delta}B - 1 + u^2 + v^2\right)$$

for some integers u,v. For this, let $\varepsilon > 2\delta$ and count the number of primes $p \leq w$ for which $2^\varepsilon | 2^{2\delta}B - 1 + p$. In fact, it is easy to show that

$$\#\{p \leq w : p \equiv 1 - 2^{2\delta}B \pmod{2^\varepsilon}\} = (1+o_w(1))\frac{\mathrm{li}(w)}{2^{\varepsilon-1}} \qquad (w \to \infty),$$

where li(w) stands for the logarithmic integral. If p is counted in the above set, then $p \equiv 1 \pmod 4$ and therefore it can be written as $p = u^2 + v^2$. Arguing the same way with $\varepsilon + 1$, we obtain that

$$\begin{aligned} \#\{p \le w : 2^\varepsilon \| p + A\} &= \#\{p \le w : 2^\varepsilon | p + A\} - \#\{p \le w : 2^{\varepsilon+1} | p + A\} \\ &= (1 + o_w(1)) \frac{\mathrm{li}(w)}{2^\varepsilon} \qquad (w \to \infty), \end{aligned}$$

a quantity which is positive if w is sufficiently large. Thus we have that $2^\varepsilon, 2^{\varepsilon+1} \in \mathcal{F}(D, A)$ if $\varepsilon > 2\delta$. We may thus conclude that

$$2 = \frac{2^{\varepsilon+1}}{2^\varepsilon} \in \mathcal{F}(D, A).$$

The proof of Theorem 2 is thus complete.

§6. The proof of Theorem 3

Since $D = 8$, we must have $Q(x, y) = x^2 + 2y^2$, with corresponding character χ defined by $\chi(1) = \chi(3) = 1$, $\chi(5) = \chi(7) = -1$. Hence $0, 1, 2, 3, 4, 6, 8 \in \mathbf{B}_8$.

First we consider the case when A is odd. In this case,

$$A, A + 1, A + 2, A + 3, A + 4, A + 6, 1 \in \mathcal{F}(8, D).$$

Now $A, A+2, A+4, A+6 \pmod 8$ alltogether give a complete reduced residue system mod 8, and consequently $\mathcal{F}(8, A) \supseteq \mathbf{Q}_2^*$. But either $2 \| A + 1$ or $2 \| A + 3$, whence $2 \in \mathcal{F}(8, D)$.

Now assume that A is even. We consider separately the cases (i) $A = 2 + 8B$, (ii) $A = 6 + 8B$, (iii) $A \equiv 4 \pmod 8$, and finally (iv) $8|A$.

In case (i), we have that $\mathcal{F}(8, A) \ni A + 1 \equiv 3 \pmod 8$, $\mathcal{F}(8, A) \ni A + 3 \equiv 5 \pmod 8$, and $1 \in \mathcal{F}(8, A)$, so that $\mathbf{Q}_2^* \subset \mathcal{F}(8, A)$. Furthermore, $A = 2(1 + 4B)$ and $1 + 4B \in \mathcal{F}(8, A)$, so that $2 \in \mathcal{F}(8, A)$, and case (i) is thus taken care of.

In case (ii), $A + 1 \equiv 7 \pmod 8$, $7 \in \mathcal{F}(8, A)$, $\mathcal{F}(8, A) \ni A = 2(3 + 4B)$, $\mathcal{F}(8, A) \ni A + 8 = 2(3 + 4(B + 1))$. One of $3 + 4B$ or $3 + 4(B + 1) \equiv 7 \pmod 8$; therefore $2 \in \mathcal{F}(8, A)$. Thus $3 + 4B = \frac{A}{2}$, $\frac{A+2}{8} = 1 + B$, $\frac{A+4}{2} = 7 + 4B$, $\frac{A+6}{4} = 3 + 2B \in \mathcal{F}(8, A)$. If B is odd, then $7 + 4B \equiv 3 \pmod 8$, thus $1, 3, 7 \in \mathcal{F}(8, A)$, which implies that $5 \in \mathcal{F}(8, A)$. If B is even, then $A = 2(3 + 4B)$ so that $3 + 4B \equiv 3 \pmod 8$ and $3 \in \mathcal{F}(8, A)$. Thus we obtain as above that $\mathcal{F}(8, A) = \mathbf{Q}^*$.

In case (iii), $A + 1 \equiv 5 \pmod 8$, $A + 3 \equiv 7 \pmod 8$; thus $1, 5, 7 \in \mathcal{F}(8, A)$, so that $3 \in \mathcal{F}(8, A)$. Hence $\mathbf{Q}_2^* \subset \mathcal{F}(8, A)$, and $2 \| A + 2$ implies that $2 \in \mathcal{F}(8, A)$, which completes case (iii).

In case (iv), we write $A = 2^\gamma B$ with $\gamma \ge 3$. Then $A + 3 \equiv 3 \pmod 8$, and $3 \in \mathcal{F}(8, A)$. We now consider separately the cases $\gamma \ge 4$ and $\gamma = 3$ with B odd. In the first case, $2 + A = 2(1 + 2^{\gamma-1}B)$, whence $2 \in \mathcal{F}(8, A)$ and therefore $B \in \mathcal{F}(8, A)$. If $B \equiv 5$ or $7 \pmod 8$, then we are done. Since $2^\nu \in \mathbf{B}_D$ for every ν, then $2^\nu + A \in \mathcal{F}(8, A)$. Thus $B, B + 1, B + 2, B + 4 \in \mathcal{F}(8, A)$. If $B \equiv 1 \pmod 8$, then $B + 2 \equiv 3 \pmod 8$ and

$B+4 \equiv 5 \pmod 8$, and we are done. If $B \equiv 3 \pmod 8$, then $B+2 \equiv 5 \pmod 8$, and we are done as well. It remains to consider the case $A = 2^3 B$ with B odd. Then $2+A = 2(1+4B)$ and $6+A = 2(3+4B)$. Since $Q(x,y)$ takes the values $2^3, 2^4, 2^5, 2^6, 3 \cdot 2^4$, it takes also the values $2^3B, 2^3(B+1), 2^3(B+2), 2^3(B+4), 2^3(B+6), 2^3(B+8)$. Since one of $B, B+2, B+4, B+6$ is $\equiv 1 \pmod 8$ and thus belongs to $\mathcal{F}(8,A)$, we have that $2^3 \in \mathcal{F}(8,A)$ and so $B, B+2, B+4, B+6 \in \mathcal{F}(8,A)$, which implies that $\mathbf{Q}_2^* \subset \mathcal{F}(8,A)$. But $2+A \in \mathcal{F}(8,A)$, and since $2 \| 2+A$, it follows that $2 \in \mathcal{F}(8,A)$, thus handling case (iv) and completing the proof of Theorem 3.