MORE ON THE SERRET–HERMITE ALGORITHM

KEITH MATTHEWS

1. Introduction

A well–known correspondence $(r, s) \rightarrow x$ between positive solutions (r, s) of $r^2 + s^2 = n$ satisfying $\gcd(r, s) = 1$ and x satisfying $x^2 \equiv -1 \pmod{n}, 1 < x < n$ is given by $xr \equiv s \pmod{n}$ in Theorem 3.1, p. 165 of Niven–Zuckerman–Montgomery. Note that $x = n/2$ implies $n = 2$, so we assume throughout that $n > 2$.

Euclid's algorithm sheds a more explicit light on the correspondence. The following result is a slight refinement of the Hermite–Serret construction which is one of the many ways of expressing a prime of the form $4n + 1$ as a sum of two squares.

2. Euclid's algorithm notation

Let $r_0 > r_1 >$, where r_1 does not divide r_0. Then we get *remainders* r_i and *quotients* q_i satisfyiing

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, \quad 0 < r_2 < r_1\\
r_1 &= r_2 q_2 + r_3, \quad 0 < r_3 < r_2\\
&\vdots\\
r_{l-2} &= r_{l-1} q_{l-1} + r_l, \quad 0 < r_l < r_{l-1}\\
r_{l-1} &= r_l q_l + r_{l+1}, \quad r_{l+1} = 0.
\end{aligned}$$

Then $r_l = \gcd(r_0, r_1)$.

We also define sequences s_i and t_i by $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$ and

$$\begin{aligned}
s_{k+1} &= -q_k s_k + s_{k-1}\\
t_{k+1} &= -q_k t_k + t_{k-1},
\end{aligned}$$

for $1 \leq k \leq l$. Then

(i) $l \geq 2$;
(ii) $q_k \geq 1$ for $1 \leq k \leq l$, with $q_l \geq 2$;
(iii) $r_k = s_k r_0 + t_k r_1$ for $0 \leq k \leq l + 1$.

Here are some other properties of the sequences r_i, s_i, t_i.

Date: 14th March 2013.

LEMMA 2.1. *For $1 \leq k \leq l$,*

$$|t_k|r_{k-1} + |t_{k-1}|r_k = r_0 \tag{1}$$

$$|s_k|r_{k+1} + |s_{k+1}|r_k = r_1 \tag{2}$$

$$s_{k-1}t_k - s_k t_{k-1} = (-1)^{k+1} \tag{3}$$

$$s_k = (-1)^k |s_k|,\ t_k = (-1)^{k+1}|t_k| \tag{4}$$

$$|s_k||t_{k+1}| - |s_{k+1}||t_k| = (-1)^k \tag{5}$$

$$|s_k| \leq r_1/2, |t_k| \leq r_0/2 \text{ if } \gcd(a,b) = 1 \tag{6}$$

$$|s_k| < |t_k| \tag{7}$$

$$0 = |s_1| < |s_2| \leq |s_3| < \cdots < |s_{l+1}| \tag{8}$$

$$1 = |t_1| < |t_2| < |t_3| < \cdots < |t_{l+1}| \tag{9}$$

Proposition 1. *Suppose x satisfies $x^2 \equiv -1 \pmod{n}$ and $1 < x < n/2$. then applying Euclid's algorithm to $r_0 = n, r_1 = x$ gives an algorithm of even length $2c$ and a decreasing sequence of remainders $r_0 > r_1 > \cdots > r_{c-1} > \sqrt{n} > r_c > \cdots > r_{2c} = 1$. Then with $r = |t_c| = r_{c+1}, s = |t_{c+1}| = r_c, a = |s_c|, b = |s_{c+1}|$, we have*

(i) $r^2 + s^2 = n$.
(ii) $1 \leq r < s, \gcd(r,s) = 1$.
(iii) $xr \equiv (-1)^{c+1}s \pmod{n}$.
(iv) $x = ar + bs$.
(v) $br - as = (-1)^{c+1}$.
(vi) $0 \leq a \leq b$.
(vii) $a \leq r/2, b \leq s/2$.
(viii) $x^2 + 1 = n(a^2 + b^2)$.

Note that a and b can be determined using (iv) and (v) and the fact that $r = r_{c+1}, s = r_c$. So r, s, a, b can be found without calculating the s_i and t_i sequences.

In the opposite direction, if $r^2 + s^2 = n$, with $1 < r < s$ and $\gcd(r,s) = 1$, we can apply Euclid's algorithm to the pair (s,r) to get the unique pair (a,b) satisfying $0 \leq a \leq b, a \leq r/2, b \leq s/2, br - as = \epsilon = \pm 1$. Then $x = ar + bs$ has the property that $x^2 \equiv -1 \pmod{n}, 1 < x < n/2$ and $xr \equiv \epsilon s \pmod{n}$.

We prove (i) and (vii) in a series of lemmas. The remaining items follow directly from Lemma 2.1. Also (viii) follows from (iv) and (v) and the identity

$$(ar + bs)^2 + (br - as)^2 = (r^2 + s^2)(a^2 + b^2)$$

and was pointed out by John Robertson.

LEMMA 2.2. (Aubry-Thue) *Let* $\gcd(a,b) = 1, a > b$. *Then the congruence*

$$bx \equiv y \pmod{a} \tag{10}$$

has a solution x, y satisfying

$$1 \leq |x| < \sqrt{a}, 1 \leq |y| \leq \sqrt{a}.$$

Proof. The remainders $r_0, r_1, , \ldots, r_m$ in Euclid's algorithm applied to $r_0 = b, r_1 = a$, decrease strictly from a to 1. Hence there exists a $k \geq 1$, such that

$$r_{k-1} > \sqrt{a} \geq r_k.$$

Then the equation $a = |t_k|r_{k-1} + |t_{k-1}|r_k$ gives

$$a \geq |t_k|r_{k-1} > |t_k|\sqrt{a}.$$

Hence $|t_k| < \sqrt{a}$. Finally,

$$r_k = s_k a + t_k b,$$

so

$$t_k b \equiv r_k \pmod{a}$$

and we can take $x = t_k, y = r_k$ in (10). □

LEMMA 2.3. (Generalization of Hermite-Serret's algorithm) *Let* $x, n \in \mathbb{N}, n > 2, x < n/2, x^2 + 1 \equiv 0 \pmod{n}$. *Perform Euclid's algorithm with* $r_0 = n, r_1 = x$. *Determine* k *by* $r_{k-1} > \sqrt{n} \geq r_k$. *Then*

$$n = r_k^2 + t_k^2.$$

Proof. In our proof of Thue's result, we saw that $r_k \equiv t_k x \pmod{n}$ with $1 \leq |t_k| < \sqrt{n}$. Then

$$\begin{aligned} r_k^2 + t_k^2 &\equiv t_k^2 x^2 + t_k^2 \\ &\equiv t_k^2(x^2 + 1) \pmod{n} \\ &\equiv 0 \pmod{n}. \end{aligned}$$

But $2 \leq r_k^2 + t_k^2 < n + n = 2n$, so $r_k^2 + t_k^2 = n$. □

LEMMA 2.4. *Let* l *be the length of Euclid's algorithm under the conditions of Lemma 2.3. Then*

$$|t_{l-i+1}| = r_i, \quad 0 \leq i \leq l + 1. \tag{11}$$

Also $l = 2c$ *and* $n = r_c^2 + r_{c+1}^2$, *where* c *is determined by the inequalities* $r_{c-1} > \sqrt{n} > r_c$.

Proof. We have $x^2 \equiv -1 \pmod{n}$. Also $1 = s_l n + t_l x$, where $|t_l| \leq n/2$. Hence

$$\begin{aligned} -x^2 &\equiv t_l x \pmod{n} \\ -x &\equiv t_l \pmod{n}. \end{aligned}$$

Hence n divides $t_l + x$. But

$$|t_l + x| \leq |t_l| + x < n/2 + n/2 = n.$$

Hence $t_l + x = 0$ and $t_l = -x$. However $t_l = (-1)^{l+1}|t_l|$, so $(-1)^{l+1} = -1$ and $l = 2c$.

Also $t_{l+1} = (-1)^l n = n$.

But we have equations

$$\begin{aligned}|t_{l+1}| &= q_l|t_l| + |t_{l-1}|\\ &\vdots\\ |t_3| &= q_2|t_2| + |t_1|\\ |t_2| &= q_1|t_1|.\end{aligned}$$

This is just Euclid's algorithm applied to $r_0 = n, r_1 = x$, as $|t_{l-1}| < |t_l|$ etc. Hence the sequences

$$|t_{l+1}|, |t_l|, \ldots, |t_1|$$

and

$$r_0, r_1, \ldots, r_l$$

are identical. i.e., $|t_{l-i+1}| = r_i, \quad 0 \le i \le l+1$.

Taking $i = c, c+1$ in (11) gives $|t_{c+1}| = r_c, |t_c| = r_{c+1}$. Then from (1), $n = |t_{c+1}|r_c + |t_c|r_{c+1} = r_c^2 + r_{c+1}^2$. Hence $r_c < \sqrt{n}$. Also

$$\begin{aligned}r_{c-1} &= q_c r_c + r_{c+1} \ge r_c + r_{c+1}\\ r_{c-1}^2 &\ge (r_c + r_{c+1})^2 > r_c^2 + r_{c+1}^2 = n.\end{aligned}$$

Hence $r_{c-1} > \sqrt{n}$. □

Finally we prove part (vii) of Proposition 1. In fact we prove

$$|s_k| \le |t_k|/2, \tag{12}$$

if $1 \le k \le l$. This is true trivially for $k = 1$ and for $k = 2$ we have $s_2 = 1, t_2 = -q_n = -q_1$ and $q_1 \ge 2$. The result extends using (5), as for $k \ge 2$, we have an alternating sum whose terms decrease in absolute value as $|t_2| < |t_3| < \cdots < |t_k|$:

$$\frac{|s_k|}{|t_k|} = \frac{1}{|t_2|} - \frac{1}{|t_2||t_3|} + \cdots + (-1)^k \frac{1}{|t_{k-1}||t_k|}. \tag{13}$$

In particular, taking $k = c$ and $c+1$ in (12) gives

$$a \le r/2, \quad b \le s/2. \tag{14}$$

Clearly we cannot have simultaneous equality in (14), as $br - as = \pm 1$.

We now give cases where equality occurs in Proposition 1.

(1) $r = 1 \iff x = s, n = 1 + s^2, s > 1$, in which case $a = 0, b = 1$.
(2) $a = 0 \iff x = s, n = 1 + s^2, s > 1$, in which case $b = 1 = r$.
(3) $a = b \iff x = 2s - 1, n = 2s^2 - 2s + 1, s > 1$, in which case $a = b = 1, r = s - 1$.
(4) $b = s/2 \iff x = 2, n = 5$, in which case $a = 0, b = 1, r = 1, s = 2$.
(5) $a = r/2 \iff x = 2b^2 + b + 2, n = 4b^2 + 4b + 5, b \ge 1$, in which case $r = 2, a = 1, s = 2b + 1$.

Example. $n = 2465$. The solutions of $x^2 \equiv -1 \pmod{2465}$ with $1 \leq x < 2465/2$ are $157, 302, 1143, 1177$.

x	a	b	r	s	c
157	1	3	16	47	3
302	1	6	8	49	4
1143	13	19	28	41	8
1177	11	21	23	44	8

See `http://www.numbertheory.org/php/hermite_serret.html` for a BC-math implementation of the algorithm in Proposition 1.