1990-1

Number Theory, *Richard A. Mollin (ed.)*

Some Conjectures Related to Fermat's Last Theorem

Andrew Granville

Dedicated to Harry Bennett on the occasion of his 90th birthday.

1. Introduction

In about 1637, Fermat claimed to have proved that for all integers $n \geq 3$, there do not exist integers x, y and z that satisfy

$$x^n + y^n = z^n \quad \text{and} \quad xyz \neq 0. \qquad (1)_n$$

This still unproved assertion, known as "Fermat's Last Theorem", has eluded the efforts of many great mathematicians (see Ribenboim's book [36] for an excellent introduction), although the many attacks to solve it have inspired much important mathematics.

The first partially successful approach was begun, in 1823, by Sophie Germain [24] who used local methods and ingenious combinatorial ideas to state results on the equation

$$x^n + y^n + z^n = 0 \quad \text{and} \quad \gcd(n, xyz) = 1 \qquad (2)_n$$

for odd integers n. She proved that if n and $2n + 1$ are both prime then $(2)_n$ has no solutions; this can be generalized as follows:

Lemma 1. ([17], [21]) *Suppose that m is a given positive even integer and S_m is the set of primes that divide some non-zero norm of the sum of three m-th roots of unity. Suppose further that p and $q = mp + 1$ are both odd primes with p not a divisor of m and $q \notin S_m$. Then, for $n = p$ (m not a multiple of 3), p^2 $(3|m)$, we have that $(2)_n$ has no solutions in integers x, y and z.*

In 1954, Ankeny and Erdős [2] used Sophie Germain's approach to show that $(2)_n$ has solutions for $o(N)$ exponents $n \le N$. More recently, Adleman and Heath–Brown [1], used Lemma 1 together with Fouvry's work on the Brun–Titchmarsh theorem [8] to show that $(2)_p$ has no solutions for infinitely many primes p. In their paper they made a number of conjectures in analytic number theory that, if proved, would in conjunction with Lemma 1, prove successively stronger theorems on the First Case of Fermat's Last Theorem (i.e., the assertion that $(2)_n$ has no solutions with $n \ge 2$).

The second successful approach was started by Kummer [22], in 1847, who introduced the concept of divisors (or ideals) and showed that $(1)_p$ has no solutions for all "regular" primes p. In 1857 Kummer [23] examined $(2)_p$ in more detail and established that if $(2)_p$ does have solutions then a complicated set of $p-2$ congruence conditions involving Bernoulli numbers and Euler polynomials must be satisfied. It was not until 1909 that Wieferich [42] ingeniously derived the following result from Kummer's congruences.

Lemma 2. *If* $(2)_p$ *has solutions in integers* x, y, z *then*

$$2^p \equiv 2 \pmod{p^2}.$$

The "Fermat quotient" is defined as $q_p(2) = \dfrac{2^{p-1}-1}{p}$, so that the conclusion of Lemma 2 can be rewritten as "p divides $q_p(2)$". The question of whether or not p divides $q_p(2)$ (or, indeed $q_p(a)$, for any integer $a \ge 2$) seems to be particularly difficult, and in Section 2 we shall examine various related conjectures. For $a = 2$, our total knowledge is that, of the primes $p < 6 \cdot 10^9$, p divides $q_p(2)$ only for $p = 1093$ and $p = 3511$ ([25]). If we assume that the "probability" that p divides $q_p(2)$ is $1/p$ (note that p divides exactly one of $q_p(2)$, $q_p(2+p), \ldots,$ $q_p(2+p(p-1))$ as $q_p(2+kp) \equiv q_p(2) - k/2 \pmod{p}$) then, of the primes $p \le x$, one expects that for about $\sum_{p \le x} 1/p \sim c + \log\log x$ such primes we have that p divides $q_p(2)$: As has been pointed out by a number of people at this conference, $\Sigma\, 1/p$ will always be less than 4 if we sum over all the primes that we know, ever will know, (or even wish to know), and so finding two primes for which p divides $q_p(2)$ is not so bad!

In 1910, Mirimanoff [31] tidied up Wieferich's long and difficult proof and extended the result to:

Lemma 3. *If* $(2)_p$ *has solutions in integers* x, y, z *then*

$$3^p \equiv 3 \pmod{p^2}.$$

In rapid succession, a number of authors proved the next few criteria (i.e., $5^p \equiv 5 \pmod{p^2}$, $7^p \equiv 7 \pmod{p^2}$, etc.), but it was not until 1914 that Frobenius [10] made an attempt to give an "algorithm" to determine each successive criteria: However, his algorithm is difficult to implement and the paper contains numerous errors. In 1917 Pollaczek [34] gave different, mostly correct proofs to determine an algorithm that allowed him to prove:

Lemma 4. *If* p *is sufficiently large and* $(2)_p$ *has solutions in integers* x, y, z *then* $q^p \equiv q \pmod{p^2}$, *for each prime* $q \le 31$.

In 1931 Morishima [33], adding a few ideas to Frobenius's paper, claimed to have extended the criteria up to $q \le 43$. However, the only proof he gave of this was to state that the computations can be done "*In analoger Weise*" to the way in which they were done up to 31. This is far from a proof, and far from a trivial assertion.

Gunderson, in his Ph.D. thesis under the supervision of Rosser [18], pointed out a number of technical errors in Morishima's paper. (Similar errors appear in the papers of both Frobenius [10] and Pollaczek [34]). Gunderson corrected these errors using some ingenious ideas. In 1988, using a more combinatorial and less algebraic approach, the author and Monagan [16] reproved the many technical theorems of Frobenius *et al.* We also proved a succession of stronger technical results and extended the above Lemmas to:

Lemma 5. *If* $(2)_p$ *has solutions in integers* x, y, z *then* $q^p \equiv q \pmod{p^2}$ *for each prime* $q \le 89$.

We also made two conjectures that, if proved, would imply that the first case of Fermat's Last Theorem is true. We shall examine these and related conjectures in Section 3.

The third important approach is due to Furtwangler [11] who used local class field theory to derive criteria, again in terms of Fermat quotients. It seems, however, that there is little to add to this approach following the recent paper of Azuhata [3]. Using this approach Hellegouarch [20] showed that if $(2)_n$ has solutions, where $n = p^t$ (p prime, $t \geq 1$) then p^{2t} divides both $2^p - 2$ and $3^p - 3$. Using this I proved in my Ph.D. thesis [15]:

Theorem 1. *For any odd prime* p, $(2)_n$ *has no solutions when* $n = p^t$ *and* $t \geq p^{1/2}/\log p$.

This improves on the many previous bounds given for t (e.g., $t \geq \phi(p - 1) \log 3 / \log p$ —see [17]).

A number of recent approaches have come from the perspective of algebraic geometry; to wit, those of Faltings [6], Frey, Ribet and Serre (see [9]). It is not my intention to discuss these here except to state the important theorem of Faltings:

Lemma 6. *For any* $n \geq 3$, *there are only finitely many triples of integers* (x, y, z) *that are coprime and satisfy* $(1)_n$.

Heath-Brown [19] and I [13] deduced from Lemma 6 that $(1)_n$ has solutions for only $o(x)$ exponents $n \leq x$.

Stewart and Tijdeman [40] observed that Lemma 6, together with the so-called "*abc* conjecture", implies that there are only finitely many solutions (x, y, z, n) to $(1)_n$ with $\gcd(x, y, z) = 1$ and $n \geq 3$. We shall discuss this further in Section 2.

2. Fermat Quotient and Powerful Numbers

We start this section with the "trendy" conjecture of number theory, due to Oesterlé and Masser [29]:

Conjecture 1. (The "abc conjecture") *Suppose that* a, b *and* c *are positive integers satisfying*

$$a + b = c \tag{3}$$

with

$$\gcd(a, b, c) = 1.$$

Let $G = G(a,b,c)$ be the product of the primes dividing abc, each to the first power. For all $\varepsilon > 0$, there exists a constant $k = k(\varepsilon)$ such that $c < kG^{1+\varepsilon}$.

(See de Weger [4] for some interesting computational information.)

Actually Oesterlé originally conjectured the existence of a constant T for which $c < G^T$ and this was sharpened by Masser. Recently Stewart and Tijdeman [40] proved a result in this direction, which they tell me can now be sharpened to $c < \exp(kG^{1+\varepsilon})$. Note that if x and y are integers and $x + y\sqrt{d}$ is a unit of $\mathbb{Q}(\sqrt{d})$, for any squarefree $d \geq 2$, and $e + f\sqrt{d} = (x + y\sqrt{d})^{2d}$ then $e^2 - df^2 = 1$ where d divides f; therefore $a = 1$, $b = df^2$, $c = e^2$ is a solution of (3) with $G(a,b,c) \leq ef \leq c/\sqrt{d}$, so that the exponent in Conjecture 1 certainly can't be improved.

Assume only Oesterlé's conjecture (i.e., $c < G^T$). Suppose that we have a solution x, y, z of $(1)_n$ with $n \geq 3T$. Let $a = x^n$, $b = y^n$, $c = z^n$ in (3) so that $G(a,b,c)^T \leq (xyz)^T < z^{3T} < z^n = c$, giving a contradiction. Thus $n < 3T$, and so, by Lemma 6, we have only finitely many quadruples (x, y, z, n) satisfying $(1)_n$ with $\gcd(x, y, z) = 1$ and $n \geq 3$.

We shall later relate Conjecture 1 directly to Fermat quotients.

As we stated in the introduction, there is very little known about the "p-divisibility" of Fermat quotients. To illustrate this we state a number of conjectures (some of these are well-known though perhaps they have never all appeared together before). We shall suppose that a is some fixed integer, with $a \geq 2$.

Conjecture 2a. *There is an odd prime p which divides $q_p(a)$.*

Conjecture 2b. *There is an odd prime p which doesn't divide $q_p(a)$.*

Conjecture 3. *There are infinitely many primes p for which p divides $q_p(a)$.*

For each integer $m \geq 2$,

Conjecture 4a)$_m$. *There are only finitely many primes p for which p^m divides $q_p(a)$.*

For each integer $m \geq 1$,

Conjecture 4b)$_m$. *There are infinitely many primes p for which p^m does not divide $q_p(a)$.*

Conjecture 5a. *Conjecture 4a)$_m$ holds for some integer $m = m(a)$.*

Conjecture 5b. *Conjecture 4b)$_m$ holds for some integer $m = m'(a)$.*

If we assume that p^m divides $q_p(a)$ with "probability" $1/p^m$ then it is easy to give a heuristic justification to each of the above conjectures.

We shall determine a number of interrelations between these conjectures, and with some others below. We first note some trivial relations between the conjectures above: If Conjecture 4a)$_m$ holds then Conjectures 4b)$_m$ and 5a hold, as well as 4a)$_n$ for each $n \geq m$. If 4b)$_m$ holds then 5b) holds as well as 4b)$_n$ for each $n \geq m$. Also Conjecture 3 implies 2a, Conjecture 4b)$_1$ implies 2b and Conjecture 5a implies 5b with $m'(a) \leq m(a)$.

Taking $a = 2$ in Conjecture 4b)$_1$ implies the theorem of Adleman and Heath-Brown (that $(2)_p$ has no solutions for infinitely many primes p), by Lemma 2. Moreover, by Hellegouarch's theorem (mentioned in the introduction), we see that Conjecture 4a)$_2$ implies that $(2)_{p^2}$ has no solutions for all but finitely many primes p; and, by Faltings' theorem (Lemma 6), this implies that there are only finitely many (n, x, y, z) satisfying $(2)_n$ with n divisible by a square and $\gcd(x, y, z) = 1$.

By generalizing an argument of Puccioni [35], I was able to show in [12] that, for any $m \geq 1$, Conjecture 4a)$_{m+1}$ implies Conjecture 4b)$_m$. (In other words if $p^m \mid q_p(a)$ for all but finitely many primes p, then $p^{m+1} \mid q_p(a)$ for infinitely many primes p.

We now make a sequence of seemingly unrelated conjectures:

Conjecture 6. (Erdős [5], Mollin and Walsh [32]) *There are only finitely many triples of consecutive powerful numbers.* (Note that n is called powerful if p^2 divides n whenever p divides n).

As noted by Mollin and Walsh, if $n-1$, n and $n+1$ are all powerful numbers then 4 divides n (as an integer $\equiv 2 \pmod 4$) can't be powerful) and so n^2-1 is powerful if and only if $n-1$ and $n+1$ are both powerful (as $\gcd(n-1, n+1) = 1$). Therefore the following is equivalent to Conjecture 6.

Conjecture 6a. *There are only finitely many even powerful numbers n such that n^2-1 is also powerful.*

In [38] Ribenboim stated the even weaker (take $n = m^2$ above):

Conjecture 6b. *There are only finitely many even integers m such that m^4-1 is also powerful.*

If A is a fixed even integer then we can take $n = A^r$ in Conjecture 6a and deduce the even weaker conjecture:

Conjecture 7a. *For every even integer A there are infinitely many values of n for which A^n-1 is not powerful.*

Actually, as $(A^{2n}-1) = (A^n-1)(A^n+1)$, we see that Conjecture 7a also follows from

Conjecture 7b. *For every even integer A there are infinitely many values of n for which A^n+1 is not powerful.*

The "link" between Conjectures 2–5 and Conjectures 6–7 comes from the following argument, which is similar to that given in [14] (we shall show that Conjecture 7a implies Conjecture $4b_1$): If Conjecture $4b_1$ is false then p divides $q_p(a)$ for all $p > p_0$. Set

$$t = \prod_{p \le p_0} \phi(p^2)$$

and $A = a^t$. It is easy to show that A^n-1 is a powerful number for all positive integers n (consider the prime divisors $p > p_0$ and $p \le p_0$ separately), and this contradicts Conjecture 7a.

In 1953, Mahler [28] proved that as $x, y \to \infty$, the largest prime factor of $x^2+y^3 \to \infty$. We make an analogous conjecture:

Conjecture 8. *The largest prime factor of* $1+x^2y^3$ *tends to infinity as* $x+|y|$ *tends to infinity.*

It is easy to show that Conjecture 8 implies Conjecture 7b: If 7b is false then A^n+1 is powerful for all sufficiently large n, i.e., $A^n+1=x^2(-y)^3$ for some x and y; and, as $n \rightarrow \infty$, this contradicts Conjecture 8.

We now show how the "*abc*" Conjecture implies both Conjecture 6a and 8:

If n and n^2-1 are both powerful then, by taking $a=1$, $b=n^2-1$ and $c=n^2$ in (3), we get $G \leq \sqrt{(bn)} < n^{3/2}$. Therefore, $n^2 < kn^{3/2+\varepsilon}$ by Conjecture 1, which bounds n, and so Conjecture 6a holds.

If x and y are integers for which the largest prime factor of $1+x^2y^3$ is $\leq t$, then take $a=1$, $b=x^2y^3$ in (3), so that $G \leq xyT$, where T is the product of primes $\leq t$. Therefore $x^2y^3 \leq c\,(xy)^{1+\varepsilon}$ where $c=kT^{1+\varepsilon}$, by Conjecture 1, which bounds xy and thus $x+|y|$. Conjecture 8 follows.

In a very recent paper Silverman [39] deduced a quantitative result on the p–divisibility of Fermat quotients from the "*abc*" Conjecture: If Conjecture 1 holds then, for any $a \geq 2$, there are $\gg \log x$ primes $p \leq x$ for which p does not divide $q_p(a)$. Actually a weaker quantitative result can be deduced from Conjecture 6a.

There are many fascinating connections between these conjectures and questions on Fermat and Mersenne numbers (see Gary Walsh's forthcoming master's thesis and also [37] and [38]); and between Fermat quotients and Bernoulli numbers (see Emma Lehmer's paper [26]).

It is also of interest to determine, for each odd prime p, an upper bound on the least integer $a=a(p)$ for which p does not divide $q_p(a)$. By D.H. Lehmer's computations ([25]) we know that $a(p) \leq 3$ whenever $p < 6 \cdot 10^9$; and H.W. Lenstra ([27]) has asserted that this is probably always the case. We are less ambitious:

Conjecture 9. *There exists an integer* N *such that for all odd primes* p, *there is a positive integer* $a \leq N$ *for which* p *does not divide* $q_p(a)$. (I.e., $a(p) \leq N$ for all odd primes p).

Conjecture 9a. (H.W. Lenstra [27]) *We may take* $N = 3$ *in Conjecture* 9.

In fact Lenstra [27] has shown that $a(p) \leq 4\log^2 p$ (subsequently reproved independently by Fouché [7]). The proof is elegant:

Define $S(x, y)$ to be the set of positive integers $\leq x$, free of prime factors greater than y. If p divides $q_p(a)$ for every $a \leq y$ then, as $q_p(\bullet)$ is an additive function (mod p), we see that p divides $q_p(a)$ for any $a \in S(p^2, y)$. However, as p divides *exactly* one of $q_p(a)$, $q_p(a+p), \ldots, q_p(a+(p-1)p)$, we see that $|S(p^2, y)| \leq p$; and so, by choosing y sufficiently large (i.e., $y = 4\log^2 p$) we get a contradiction.

By considering the set $S^*(p, y)$ of quotients m/n of coprime integers m, n from $S(p, y)$ it is possible to improve the above to $a(p) \leq \log^2 p$; and, by a similar method, Tanner and Wagstaff [41] have shown, as a corollary to Lemma 5, that $(2)_n$ has no solutions for $n \leq 1.564 \times 10^{17}$. More recently, Coppersmith [43] has come up with a new method that gives $n \leq 7.568 \times 10^{17}$; however, in general, Coppersmith's method also gives $a(p) \leq \log^2 p$.

As we shall see in the next section, we would like to improve these results to

Conjecture 10. *For any constant* $c > 0$, *if* p *is sufficiently large then* $a(p) \leq c(\log p)^{1/4}$.

This would seem to require a genuinely new idea. I have been unable to prove even the existence of infinitely many primes p for which $a(p) \leq (\log p)^{2-\varepsilon}$, for some $\varepsilon > 0$.

We now give

Proof of Theorem 1. Hellegouarch [20] showed that if $(2)_n$ has solutions then p^{2t} divides both $2^{p-1} - 1$ and $3^{p-1} - 1$. If $x = 2^a 3^b$ or $1/2^a 3^b$ or $2^a/3^b$ or $3^b/2^a$ where a and b are non–negative integers then it is easy to show that $x^{p-1} \equiv 1 (\mathrm{mod}\ p^{2t})$; and, if both numerator and denominator are $< p^t$ then these integers are distinct (mod p^{2t}). Gunderson [18] showed that the number of such integers is

$$\geq 1 + \frac{3\log^2 n - (\log 12)\log n}{\log 2 \log 3}. \tag{4}$$

However, as there are exactly $p-1$ distinct solutions $(\bmod\, p^{2t})$ of $x^{p-1} \equiv 1 (\bmod\, p^{2t})$, we have a contradiction if the quantity in (4) is $\geq p$. This clearly occurs if $t \geq p^{1/2}/\log p$.

3. Some Matrices

The purpose of this section is to expand upon the conjectures given in [16]. First I will give a vague outline of the previously mentioned method of Frobenius *et al.*: For integers a, b, c with $c > 0$ and $\gcd(b,c) = 1$ define $\alpha(a,b,c)\,(\beta(a,b,c))$ to be the least positive (non–negative) residue of $a/b\ (\bmod\, c)$.

Let $A_n(t)$ be the $2n$ by n matrix with (i,j)th entry

$$t^{\alpha(j,n,i)} \text{ (if } \gcd(ij,n) = 1\text{)}, \ 0 \text{ (otherwise)}.$$

If (x,y,z) is a solution of $(2)_p$ then define $H = H(x,y,z)$ to be the set of congruence classes $(\bmod\, p)$ of $-x/y$, $-y/x$, $-y/z$, $-z/y$, $-x/z$, $-z/x$. Note that if $t \in H$ then

$$H = \{t, 1-t, t^{-1}, 1-t^{-1}, t/(t-1), 1/(1-t)\}. \tag{5}$$

The main theorem of Frobenius *et al.* states

Lemma 7. *Suppose that $t \in H$ and n is a positive integer for which*

(i) *The matrix $A_m(t)$ has rank $\phi(m)$ in the ring $\mathbb{Z}/p\mathbb{Z}$, for each m in the range $1 \leq m \leq n$.*

(ii) *t has order $\geq 2n+1$ $(\bmod\, p)$.*

Then p^2 divides $q^p - q$ for all primes $q \leq 2n+1$.

Gunderson [18] gave the first correct proof that t cannot have order 3, 4 or 6 $(\bmod\, p)$. From this and a result of Pollaczek one can derive:

Lemma 8. *There exists a constant $c_1 > 0$ such that if $(2)_p$ has solutions then there exists $t \in H$ which has order $> c_1(\log p)^{1/2}$ $(\bmod\, p)$.*

Lemma 8 makes it easy to satisfy Lemma 7 (ii) and so the real difficulty in implementing Lemma 7 is in proving that the criteria in Lemma 7 (i) hold for each successive integer m. In practice, we do not know much about $t \in H$ except that it is not $\equiv 0 \pmod{p}$ and can have reasonably high order (by Lemma 8). Thus we have to prove Lemma 7 (i) by taking determinants of $\phi(m)$ by $\phi(m)$ submatrices of $A_m(\acute{X})$ and examining these polynomials.

Let us suppose that $A_m(t)$ does indeed have rank $\phi(m)$ in $\mathbb{C}$ for any complex number t, except when $t \in U$ $(=\{0\} \cup \{\text{the roots of unity}\})$. We shall prove that there exists a constant $c_2 > 0$ such that if $\log p > c_2 m^4$ then $A_m(t)$ has rank $\phi(m)$ in $\mathbb{Z}/p\mathbb{Z}$:

First note that as each entry of $A_m(t)$ has degree $\leq 2m$ thus

$$\text{Any subdeterminant of } A_m(t) \text{ has degree } \leq 2m^2. \tag{6}$$

Now suppose that $A_m(t)$ has rank $< \phi(m)$ in $\mathbb{Z}/p\mathbb{Z}$. Then each non-zero $\phi(m)$ by $\phi(m)$ subdeterminant D of $A_m(x)$ is divisible by an irreducible polynomial $f_D(x)$ such that $f_D(t) \equiv 0 \pmod{p}$. By hypothesis, either $f_D(x)$ is a cyclotomic polynomial, or we get two distinct polynomials g_1 and g_2 with $g_1(t) \equiv g_2(t) \equiv 0 \pmod{p}$.

If f is a cyclotomic polynomial then, by (6), t has order $\leq 2m^2 \ll (\log p)^{1/2}$, which contradicts Lemma 8 if c_2 is chosen sufficiently small.

As the matrix $A_m(t)$ has got monomial entries with coefficients 1, we see that, for any subdeterminant D, the sum of the absolute values of the coefficients is bounded by $m!$. By a method of Mignotte [30] this means that for any g dividing D we have

$$\|g\|_2 \leq 2^{2m^2} m!$$

(by (6)), where $\|g\|_2 = \left(\sum_{i=0}^{d} g_i^2\right)^{1/2}$ and $g(x) = \sum_{i=0}^{d} g_i x^i$.

We have two such (distinct) polynomials g_1 and g_2, and as they have no common root, we know that p divides their resultant (as p divides $g_1(t)$ and $g_2(t)$). Therefore, by using the standard bounds for the determinant of a matrix we have

$$p \le \|g_1\|_2^{\deg g_2} \|g_2\|_2^{\deg g_1} \le (2^{2m^2} m!)^{4m^2} < \exp(c_3 m^4)$$

giving a contradiction.

Observing that we have already chosen t with order $\ge 2n+1 \pmod p$ we see that we have proved the following:

Theorem 2. *Suppose that $A_m(t)$ has rank $\phi(m)$ in $\mathbb{C}$ for any complex number t, not in U, and for any m, $1 \le m \le n$. There exists a constant $c_2 > 0$ such that if $p > \exp(c_2 n^4)$ and $(2)_p$ has solutions then p^2 divides $q^p - q$ for each $q \le 2n+1$.*

(In [16] the constant c_2 is given explicitly.) So what we really wish to prove is

Conjecture 11. *For any complex number t, $t \notin U$, and for any positive integer n, the matrix $A_n(t)$ has rank $\phi(n)$.*

As a corollary to Theorem 2 we have

Corollary 1. *If Conjectures 10 and 11 are true then the first case of Fermat's Last Theorem is true for all sufficiently large exponents.*

Suppose that $\gcd(m,n) = 1$ and consider using the Euclidean algorithm in $\mathbb{Z}[t,x]$ to eliminate the variable x from $1 - x^m$ and $1 - tx^n$. It is easy to see that there exist polynomials $U_m(x)$ and $V_m(x)$ of degree $\le n-1$, $\le m-1$, respectively, such that

$$t^m - 1 = (1 - x^m)U_m(x) - (1 - tx^n)V_m(x) \tag{7}$$

Explicitly we can show that

$$U_m(x) = \sum_{i=0}^{n-1} t^{\alpha(i,n,m)} x^i$$

and

$$V_m(x) = \sum_{j=0}^{m-1} t^{\beta(j,n,m)} x^j.$$

We thus see that the entries of $A_n(t)$ appear in a natural way as the coefficients of $U_m(x)$!!

It may well turn out to be easier to approach Conjecture 11 by considering the following equivalent Conjecture:

Conjecture 12. *Let $B_n(t)$ be the $2n$ by n matrix with (i, j)th entry*

$$\frac{1}{(t^i - \alpha^{ij})}$$

where α is a primitive n-th root of unity. For every positive integer n and complex number $t \notin U$, the matrix $B_n(t)$ has full rank.

Theorem 3. *Conjecture 11 holds if and only if Conjecture 12 holds.*

A proof of Theorem 3 can be found in [15]; the main idea comes from substituting $x = \tau$ in (7) for $\tau^n = t^{-1}$, so that $U_m(\tau) = -(1 - t^m)/(1 - \tau^m)$. Letting $\rho = \tau_0^{-1}$, for a fixed root τ_0 of $X^n = t^{-1}$, we see that if $\tau = \tau_0\alpha^j$ then

$$U_m(\tau)/\rho^m(t^m - 1) = 1/(\rho^m - \alpha^{jm})$$

and so we can compare the matrices $B_n(\rho)$ and $A_n(t)$.

References

[1] *L.M. Adleman* and *D.R. Heath-Brown*, The first case of Fermat's last theorem. Invent. Math., 79 (1985), 409—416.

[2] *N.C. Ankeny* and *P. Erdős*, The insolubility of classes of diophantine equations. Amer. J. Math., 76 (1954), 488—496.

[3] *T. Azuhata*, On Fermat's Last Theorem. Acta Arith., 45 (1985), 19—27.

[4] *B. de Weger*, Solving exponential diophantine equations using lattice basis reduction algorithms. J. Number Theory, 26 (1987), 325—367.

[5] *P. Erdős*, Problems and results on consecutive integers. Eureka, 38 (1975/6), 3—8.

[6] *G. Faltings*, Endlichkeitssätze für Abelsche Varietaten über Zahlkonpern. Invent. Math., 73 (1983), 349—366.

[7] *W.L. Fouché,* On the Kummer–Mirimanoff congruences. Quart. J. Math., **37** (1986), 257—261.

[8] *E. Fouvry,* Théorème de Brun–Titchmarsh; application au théorème de Fermat. Invent. Math., **79** (1985), 383—407.

[9] *G. Frey,* Links between stable elliptic curves and certain diophantine equations. Ann. Univ. Saraviensis, **1** (1986), 40pp.

[10] *G. Frobenius,* Über den Fermatschen Satz III. Sitzungsber. Akad. d. Wiss. zu Berlin, (1914), 653—681.

[11] *P. Furtwängler,* Letster Fermatschen Satz und Eisentstein'sches Reziprositätsgesetz. Sitzungsber. Akad. d. Wiss. Wien. Abt. IIa, **121** (1912) 589—592.

[12] *A. Granville,* Refining the conditions on the Fermat quotient. Math. Proc. Camb. Phil. Soc., **98** (1985), 5—8.

[13] *A. Granville,* The set of exponents for which Fermat's Last Theorem is true, has density one. C.R. Math. Acad. Sci. Canada, **7** (1985), 55—60.

[14] *A. Granville,* Powerful numbers and Fermat's Last Theorem. C. R. Math. Acad. Sci. Canada, **8** (1986), 215—218.

[15] *A. Granville,* Diophantine equations with varying exponents (with special reference to Fermat's Last Theorem). Thesis, Queen's University, (1987).

[16] *A. Granville* and *M.B. Monagan,* The First Case of Fermat's Last Theorem is true for all prime exponents up to 714,591,416,091,389. Trans. Amer. Math. Soc., **306** (1988), 329—359.

[17] *A. Granville* and *B. Powell,* Sophie Germain Type criteria for Fermat's Last Theorem. Acta Arith., **50** (1988), 265—277.

[18] *N.G. Gunderson,* Derivation of Criteria for the First Case of Fermat's Last Theorem and the Combination of these Criteria to Produce a New Lower Bound for the Exponent. Thesis, Cornell University, (1948).

[19] *D.R. Heath-Brown,* Fermat's Last Theorem for "almost all" primes. Bull. London Math. Soc., **17** (1985), 15—16.

[20] *Y. Hellegouarch,* Courbes Elliptique et Equation de Fermat. Thesis, Besançon, (1972).

[21] *M. Krasner,* A propos du critère de Sophie Germain–Fertwängler pour le premier cas du théorème de Fermat, Mathematica Cluj, **16** (1940), 109—114.

[22] *E.E. Kummer,* Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ. Monatsber. Akad. d. Wiss., Berlin, (1847) 132—139, 140—141, 305—319.

[23] *E.E. Kummer,* Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^{\lambda} = 1$ gebildeten complexen Zahlen, für den Fall dass die Klassenzahl durch λ theilbar ist, nebst Anwendungen derselben auf einen weiteren Beweis des letztes Fermat'schen Lehrsatzes. Math. Abhandl. Akad. d. Wiss., Berlin, (1857), 41—74.

[24] *A.M. Legendre,* Sur quelques objets d'analyse indéterminée et particuliérement sur le théorème de Fermat. Mém. de l'Acad. des Sciences, Institut de France, **6** (1823) 1—60.

[25] *D.H. Lehmer,* On Fermat's quotient, base two. Math. Comp., **36** (1981), 289—290.

[26] *E. Lehmer,* On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson. Ann. of Math., **39** (1938), 350—360.

[27] *H.W. Lenstra Jr.,* Miller's primality test. Inform. Proc. letters, **8** (1979), 86—88.

[28] *K. Mahler,* On the greatest prime factor of $ax^m + by^m$. Neiuw. Arch. Wiskunde, **1** (1953), 113—122.

[29] *D.W. Masser,* Open problems. Proc. Symp. Analytic Number Thy., *W.W.L. Chen* (ed.), London: Imperial Coll., (1985).

[30] *M. Mignotte,* Some useful bounds. Algebra, Symbolic and Algebraic Computation, New York, Springer-Verlag, (1983), 259—263.

[31] *D. Mirimanoff,* Sur le dernier théorème de Fermat. C. R. Acad. Sci. Paris, **150** (1910), 204—206.

[32] *R.A. Mollin* and *P.G. Walsh,* A note on powerful numbers, quadratic fields and the Pellian. C. R. Math. Acad. Sci. Canada, **8** (1986), 109—111.

[33] *T. Morishima,* Über die Fermatsche Quotienten. Jpn. J. Math., **8** (1931), 159—173.

[34] *F. Pollaczek,* Über den grossen Fermat'schen Satz. Sitzungsber. Akad. d. Wiss. Wien, Abt. IIa, **126** (1917), 45—59.

[35] *S. Puccioni,* Un teorema per una resoluzioni parziali del famoso problema di Fermat. Archimede, **20** (1968), 219—220.

[36] *P. Ribenboim,* 13 Lectures on Fermat's Last Theorem. New York, Springer-Verlag, (1979).

[37] *P. Ribenboim,* The Book of Prime Number Records. New York, Springer-Verlag, (1988).

[38] *P. Ribenboim,* Impuissants devant les puissances. Expo. Math., **6** (1988), 3—28.

[39] *J. Silverman,* Wieferich's Criterion and the *abc*–Conjecture. J. Number Theory, **30** (1988), 226—237.

[40] *C.L. Stewart* and *R. Tijdeman,* On the Oesterlé–Masser Conjecture. Monatsh. Math., **102** (1986), 251—257.

[41] *J.W. Tanner* and *S.S. Wagstaff Jr.,* New bound for the first case of Fermat's Last Theorem. Preprint.

[42] *A. Wieferich,* Zum letzten Fermat'schen Theorem. J. reine u. angew. Math., **136** (1909), 293—302.

[43] *D. Coppersmith,* Fermat's Last Theorem (Case 1) and the Weiferich Criterion. Preprint.

Department of Mathematics, University of Toronto, Toronto, Ontario, CANADA M5S 1A1.