A second note on Fermat's conjecture.

To Professor László Kalmár on his 50th birthday.

By P. DÉNES and P. TURÁN in Budapest.

1. In a previous note[1]) one of us proposed the following problem. Let q be a fixed odd prime and we consider $R_q(N)$ the number of integer (x, y, z)-solutions of the equation

$$x^q + y^q = z^q \tag{1.1}$$

with

$$1 \leqq x, y, z \leqq N \tag{1.2}$$

and

$$(x, y) = (x, z) = (y, z) = 1. \tag{1.3}$$

If Fermat's conjecture is true, then $R_q(N) = 0$; the proposed problem consists in finding *upper estimations* for $R_q(N)$. The number of systems with (1.2) is N^3; the first non-trivial estimation in[1]) was

$$R_q(N) < c_1 N \log^{\frac{1}{q-1}} N, \tag{1.4}$$

where c_1 depends only upon q. In this note we give two more upper estimations; we shall show by elementary means the better estimation

$$R_q(N) < q\left(1 + 3.2^{\frac{1}{q}}\right) N^{\frac{2}{q}}, \tag{1.5}$$

and afterwards, using deeper tools, the estimation

$$R_q(N) < c_2(q) \frac{N^{\frac{2}{q}}}{\log^{2-\frac{2}{q}} N}. \tag{1.6}$$

It is very probable that to prove the inequality

$$R_q(N) < c_3 N^{\frac{1}{q}} \tag{1.7}$$

---

[1]) P. TURÁN, A note on Fermat's conjecture. *J. Indian Math. Soc.*, **15.** (Part A), (1951), 47—50. — Here as well as in the quoted paper solutions (a, b, c) and (b, a, c) with $a \neq b$ are always counted as distinct ones.

is within the possibilities; concerning that see **6.** A proof of

(1. 8) $$R_q(N) < c_4(\varepsilon) N^{\varepsilon}$$

for arbitrarily small positive ε seems to be however very deep.

2. We denote by $R'_q(N)$ the number of solutions of (1. 1) satisfying the additional condition

(2. 1) $$(x, q) = (y, q) = (z, q) = 1.$$

Let us consider first $R'_q(N)$. We write

(2. 2) $$(z-x)\frac{z^q - x^q}{z-x} = y^q.$$

We suppose p to be a prime, $p \neq q$ and

(2. 3) $$p \mid (z-x),$$

moreover

(2. 4) $$p \left| \left(\frac{z^q - x^q}{z-x} \right) \right..$$

From (2.3) and (2.4) we obtain

$$0 \equiv \frac{z^q - x^q}{z-x} \equiv q z^{q-1} \pmod{p},$$

i. e. $p \mid z$. But (2. 3) gives then $p \mid x$, i. e. $(x, z) > 1$, a contradiction to (1. 3). Thus the greatest common divisor of $(z-x)$ and $\frac{z^q - x^q}{z-x}$ could only be q; but from (2. 2) this would mean $q \mid y$ which contradicts to (2. 1). This means that

$$\left(z-x, \frac{z^q - x^q}{z-x} \right) = 1,$$

i. e. with a positive integer a

(2. 5) $$z - x = a^q.$$

What an upper limitation can be given for a? From (2.5) and (1.2) we get

$$a^q < z \leqq N,$$

i. e.

(1. 6) $$a < N^{\frac{1}{q}}.$$

A similar reasoning gives also

$$\left(z-y, \frac{z^q - y^q}{z-y} \right) = 1,$$

i. e. with a positive integer b

(2. 7) $$z - y = b^q,$$

(2. 8) $$b < N^{\frac{1}{q}}.$$

Thus the values of a and b can be chosen at most on $N^{\frac{2}{q}}$ ways. Fixing such a pair

$$x = z - a^q, \quad y = z - b^q,$$

we get from (1.1)

$$(z-a^q)^q + (z-b^q)^q = z^q.$$

Hence the number of z-values — and at the same time that of the (x, y, z) -solutions — is at most q, i. e.

$$R'_q(N) < q N^{\frac{2}{q}}. \tag{2.9}$$

3. Next we consider $R''_q(N)$, the number of the solutions of (1. 1) with

$$q \mid xyz. \tag{3.1}$$

(1. 3) gives that only one of x, y, z is divisible by q; suppose $q \mid x$. Then

$$(y, q) = (z, q) = 1$$

and writing the equation (1. 1) in the forms

$$(z-x)\frac{z^q - x^q}{z-x} = y^q,$$

$$(x+y)\frac{x^q + y^q}{x+y} = z^q,$$

the reasoning of **2.** can be repeated. Thus with positive integer a and b we get

$$z - x = a^q,$$

$$x + y = b^q$$

and

$$a^q < z \leqq N, \qquad a < N^{\frac{1}{q}},$$

$$b^q \leqq 2N, \qquad b \leqq (2N)^{\frac{1}{q}},$$

Hence the contribution of the solutions with q/x is

$$< q(2N^2)^{\frac{1}{q}},$$

i. e.

$$R''_q(N) < 3q \cdot 2^{\frac{1}{q}} \cdot N^{\frac{2}{q}}. \tag{3.2}$$

(2.9) and (3.2) prove the inequality (1.5).

4. The proof of (1. 6) is deeper. It is based on the following theorem of Furtwängler[2]). For every (x, y, z)-solution of the equation (1.1) with (1.3)

[2]) P. Furtwängler, Letzter Fermat'scher Satz und Eisensteinsches Reciprocitätsgesetz. *Sitzungsberichte Akad. Wiss. Wien* **121** (1912), p 589—592. — In fact, this is only a special case of what he actually proved.

holds that, if u is one of x, y, z which is not divisible by q, then u is built up exclusively of such p primes for which

$$p^{q-1} \equiv 1 \pmod{q^2}. \tag{4.1}$$

It is easy to see that the p-primes satisfying (4.1) are contained in $(q-1)$ arithmetical progressions mod q^2

$$\begin{aligned} p &\equiv l_1 \quad (=1) \pmod{q^2} \\ &\vdots \qquad\qquad \vdots \\ p &\equiv l_{q-1} \pmod{q^2}. \end{aligned} \tag{4.2}$$

Indeed, if m is a primitive root mod q^2 and the p-primes satisfying (4.1) are written in the form

$$p \equiv m^k \pmod{q^2},$$

then

$$m^k(q-1) \equiv 1 \pmod{q^2}$$

and, since m is a primitive root mod q^2, we get $q \mid k$, i. e.

$$k = q, 2q, \ldots, (q-1)q.$$

This proves (4.2); we shall use Furtwängler's theorem in this form.

5. We consider again $R'_q(N)$. The a in (2.5) is a divisor of y and thus we know about a not only that $a \leqq N^{\frac{1}{q}}$, but, owing to (4.2), since $(y, q) = 1$, that a is composed exclusively of p primes satisfying (4.2). Let $a_1 < a_2 < \ldots$ be all positive integers composed of the progressions (4.2). If $s = \sigma + it$ is the complex variable, then we have for $\sigma > 1$

$$F(s) = \sum_{\nu} \frac{1}{a_\nu^s} = \prod_{\nu=1}^{q-1} \prod_{p \equiv l_\nu \pmod{q^2}} \frac{1}{1 - \frac{1}{p^s}}. \tag{5.1}$$

Standard theorems in the theory of L-functions of Dirichlet show the existence of functions $f_\nu(s)$ regular in the domain

$$\sigma > 1 - \frac{1}{\log(2 + |t|)}$$

and satisfying here an inequality

$$|f_\nu(s)| \leqq \exp\left\{c_5(\varepsilon, q) \frac{\log(3+|t|)}{\log\log(3+|t|)}\right\}$$

such that

$$\begin{aligned} F(s) &= f_1(s) \exp\left\{\sum_{\nu=1}^{q-1} \sum_{p \equiv l_\nu \pmod{q^2}} \frac{1}{p^s}\right\} = \\ &= f_1(s) \exp\left\{\sum_{\nu=1}^{q-1} \frac{1}{q(q-1)} \sum_{\chi \pmod{q^2}} \overline{\chi}(l_\nu) \log L(s, \chi)\right\} = \\ &= f_2(s) \exp\left\{\sum_{\nu=1}^{q-1} \frac{1}{q(q-1)} \log L(s, \chi_0)\right\} = \frac{f_3(s)}{(s-1)^{\frac{1}{q}}}. \end{aligned}$$

A standard technique shows then for $Y \to \infty$

$$\sum_{a_\nu \leqq Y} 1 \sim c_6(q) \frac{Y}{\log^{1-\frac{1}{q}} Y}.$$

Hence the number of the possible a-values is $\left(\text{with } Y = N^{\frac{1}{q}}\right)$

$$< c_7(q) \frac{N^{\frac{1}{q}}}{\log^{1-\frac{1}{q}} N}$$

and thus repeating the reasoning of **2**, we get

$$R_q'(N) < c_8(q) \frac{N^{\frac{2}{q}}}{\log^{2-\frac{2}{q}} N}.$$

A similar change in the reasoning in **3** gives at once

$$R_q''(N) < c_9(q) \frac{N^{\frac{2}{q}}}{\log^{2-\frac{2}{q}} N},$$

which proves (1. 6).

6. We return to (2. 5). Fixing the value of a we get from (1. 1)

(6. 1) $$x^q + y^q = (x + a^q)^q.$$

Denoting the number of the positive integer solutions of (6. 1) with $x, y \leqq N$ by $f(N,a)$ we get

(6. 2) $$R_q'(N) < \sum_{a < N^{1/q}} f(N, a).$$

If one could show that the number of solution of (6. 1) is $O(N^\varepsilon)$ then (6. 2) would give at once

$$R_q'(N) < c_{10}(q, \varepsilon) N^{\frac{1}{q}+\varepsilon}$$

and slight changes would result also $R_q(N) < c_{11}(q, \varepsilon) N^{\frac{1}{q}+\varepsilon}$.

(Received December 1, 1954.)