**Zeitschrift:** L'Enseignement Mathématique
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique
**Band:** 62 (2016)
**Heft:** 1-2

**Artikel:** Solution of the Ree group problem : a lecture at Rutgers University in 1979
**Autor:** Bombieri, Enrico
**DOI:** https://doi.org/10.5169/seals-685366

*L'Enseignement Mathématique* (2) 62 (2016), 301–311 DOI 10.4171/LEM/62-1/2-16

# Solution of the Ree group problem
# A lecture at Rutgers University in 1979

Enrico Bombieri

**Mathematics Subject Classification (2010).** Primary: 20D05, 12E20.

**Keywords.** Ree groups, classification of finite simple groups, automorphims of finite fields.

The history of the Ree groups is an interesting one. Everything began in 1960–61 when Suzuki, in the process of investigating a class of doubly transitive groups, discovered a new series of simple groups whose existence was hitherto unsuspected.

In 1961, Ree discovered that the Suzuki groups could be interpreted as "unusual twisted forms" of the orthogonal groups over a field of characteristic 2, the existence of the twisting being peculiar to this characteristic. More usual forms of twisting had been discussed earlier by Steinberg. Thus the Suzuki groups became the groups ${}^2B_2(2^{2n+1})$. Now Ree found that the exceptional Lie groups $G_2$ and $F_4$ also gave rise to new families of twisted groups, in characteristic 3 and 2 respectively. If one tries to characterize the ${}^2G_2(3^{2n+1})$ by means of simple properties, one notes that

(i) the 2-Sylow subgroups of $G$ are abelian.

(ii) According to Brauer theory, centralizers of involutions can be used to characterize simple groups. $G$ has only one class of involutions and there is an involution $w$ such that

$$C_G\big(\langle w\rangle\big) \cong \langle w\rangle \times \mathrm{P}SL(2,q), \quad q = 3^{2n+1}.$$

(iii) $G$ has no subgroup of index 2.

**Definition 1.** A group of Ree type is a group satisfying (i), (ii), (iii), $q > 5$.

The main point is: *Every group of Ree type is a simple group*. Hence if we want to find all finite simple groups we must determine all groups of Ree type.

**Theorem 2.** *Every group of Ree type is one of the Ree groups.*

In this talk I want to explain why, without knowing anything of finite group theory, I got interested in this problem. When accepting to give this talk, I had to decide whether to give a technical resumé of my proof, pointing out the way one overcomes difficult points, or give an exposition on how one arrives at certain ideas. Since in my opinion the technical content of my work is rather limited, while the major difficulty consists in realizing how useful actually is the scant information available to us, I opted for the latter choice.[1]

My first contact with Ree groups was in 1973, when John Thompson gave a lecture on the problem, at the Collège de France (Paris). After his talk, Thompson told me that he had reduced the problem to a question about automorphisms of finite fields. He even wrote it for me at dinner on a paper napkin, and I spent half a night looking at a seemingly innocuous problem and discovering that the more I tried the more difficult it became.

I got interested in Ree groups again last March.[2] Two main reasons: a group theory year at IAS and the presence of Danny Gorenstein. So when his report on the status of the classification of finite simple groups appeared in a long memoir in the Bullettin of the American Mathematical Society, I tried to read it (with mixed success) and at last arrived to page 117 where it mentions the problem again, ending with "Let me emphasize that to work on this problem requires only a rudimentary knowledge of finite group theory, for it quickly reduces to specific combinatorial questions about functional equations with coefficients in $GF(3^n)$. Hopefully this discussion will tempt some "nonspecialist" to consider the problem."

I was a nonspecialist, therefore I was qualified to consider the problem; also I was tempted once more. (Maybe it was a challenge!) The next step: Go to the library and check what the problem was.

Before presenting the problem and explaining how you solve it, I would like to say a few words on how it got reduced to a question in elementary algebra. Firstly, Ward in his 1962 thesis, imposing a couple of technical conditions (e.g. the Sylow 2-subgroups $S_2$ are elementary abelian of order 8; if $x \in C_G(\langle w \rangle)$ and $(6, |\langle x \rangle|) = 1$ then $C_G(\langle x \rangle) \leqq C_G(\langle w \rangle)$ showed that

(A) $q = 3^{2n+1}$.

(B) $G$ is simple.

A further partial step was obtained in the meantime by Landrock and Michler showing that Hall subgroups of order $q \pm 3\sqrt{\frac{q}{3}} + 1$ are cyclic $\Rightarrow$ uniqueness

[1] The technical exposition is in E. Bombieri, Thompson's problem ($\sigma^2 = 3$). Appendices by A. Odlyzko and D. Hunt, *Invent. Math.* **58** (1980), 77–100.

[2] March 1979.

of character table.

(C) The character table of $G$ is almost fully determined.

(D) The $S_3$-subgroups $P$ have $|P| = q^3$, $[P, P]$ elementary of order $q^2$, $Z(P) = [P, P, P]$ elementary of order $q$, if $p \in [P, P] - Z(P)$ then $C_P(p) = [P, P]$, if $p \in P - [P, P]$ then $C_P(p) = \langle p, Z(P)\rangle$, and if $|\langle p\rangle| = 3$ then $p \in [P, P]$.

(E) $G$ is a doubly transitive group.

(F) further information about the normalizer $N_G(P)$.

Ward's results exploit character theory. By a delicate piece of local analysis, Janko and Thompson removed the technical conditions in Ward's theorem. Moreover, the analysis in the case $q = 4$ (or $q = 5$) led Janko to the discovery of the first new sporadic group $J_1$!

Now it is useful to compare this situation with the one encountered by Suzuki. What Suzuki did was:

($\alpha$) determine the $S_2$-subgroup structure as in (D);

($\beta$) find all 2-groups with the same structure, they are determined up to an automorphism of $GF(2^{2n+1})$;

($\gamma$) use the fact that $G$ contains the group ${}^2B_2(2)$ in a certain way to infer that a certain compatibility condition on the automorphism has to be satisfied;

($\delta$) determine the automorphism;

($\varepsilon$) determine the group.

If one wanted to proceed in this way, (by Ward, Janko, and Thompson) the first step ($\alpha$) was done.

Then Thompson proceeded to obtain the other steps. Being in characteristic 3, everything was triply difficult. Step ($\beta$) was not too hard. I could almost follow Thompson. It is a standard way of analyzing the lower central series of a $p$-group by means of Lie algebras in char $p$. See Gorenstein's book Finite Groups. Here the $S_3$-Sylow $P$ is identified with triples $(a, b, c)$ such that $a, b, c \in GF(3^{2n+1})$ and

$$\begin{aligned} &(a, b, c)(\alpha, \beta, \gamma) \\ (*) \quad &= (a + \alpha, b + \beta + a\alpha^\sigma - a^\sigma\alpha, c + \gamma + \alpha b + a^\sigma\alpha^2 + a\alpha^{1+\sigma} - a^2\alpha^\sigma) \end{aligned}$$

where $\sigma \in \mathrm{Aut}\big(GF(3^{2n+1})\big)$.

Equation (*) implies that $\sigma$ generates $\mathrm{Aut}\big(GF(3^{2n+1})\big)$. From the structure of $N_G(P)$, Thompson shows that there is an integer $b$ such that

$$x^{b(\sigma+2)} = x \quad \text{in} \quad GF(3^{2n+1});$$

also $\sigma$ being a generator implies that there is an even integer $a$ such that

$$x^{a(\sigma+1)} = x^2 \quad \text{in} \quad GF(3^{2n+1}).$$

Step $(\gamma)$ is unbelievably complicated and the calculations are extremely hard. However, at the end Thompson emerges with $\sigma$ and $d \in GF(3^{2n+1})$, and a certain identity in $P$. It is implicit in Thompson that $\sigma, d$ determine $G$. This was done explicitly by Hopkins, who proved $d = 0, 1$ or $-1$ and $\sigma$ determines $d$, hence $G$.

I will refrain from writing Thompson's identity, but I have to write down the simplest consequence Thompson could obtain.

**Thompson's condition.** *$\sigma$ has the following non-trivial property. Let $z$, $y$, $u$ be in $GF(3^{2n+1})$ and suppose that $z \neq 0$ and*

$$\begin{cases} z^{\sigma+2} - y^{\sigma+2} = -1 \\ z^{\sigma+1} - y^{\sigma+1} = u. \end{cases}$$

*Then*[3]

$$z(u-1)^a - (z - y + 1)u^a - y(u+1)^a + (u^2-1)^a = 0.$$

Let us leave aside Step $(\delta)$.

Then Thompson proceeded to show

(i) Ree groups have $\sigma^2 = 3$;

(ii) if $\sigma^2 = 3$ then $d = 0$ and $G$ is a Ree group.

Thus it remains:

Step $(\delta)$: Thompson's identity implies $\sigma^2 = 3$.

I will describe now how you prove $(\delta)$. I want to point out that in order to study the problem one does not need any knowledge of group theory.

The main difficulty is psychological: What kind of attitude do you take trying to solve a problem?

First of all, we have three equations in three unknowns and formally, $a = \frac{2}{\sigma+1}$. If everything is well, we get finitely many solutions $(z, y, u)$. However, one checks easily with Thompson that $(z, y, u)$ has exactly $3^{2n+1}$ possibilities. Thus $n$ cannot be too large unless something "special" happens and "special" should mean $\sigma^2 = 3$. Hence our philosophy is: either $\sigma^2 = 3$ or $q = 3^{2n+1}$ is small.

---

[3] Note that $z = 0$ implies $y = 1$ and $u = -1$, thus getting a trivial solution valid for all $\sigma$, so we should exclude solutions with $z = 0$ from our considerations.

Next, $a$ is defined in a most implicit way and one would like to get rid of it. Here it is how:

$$\sigma \textit{ is an automorphism } \Rightarrow \textit{ more equations.}$$

Apply $\sigma$. Now

$$z^\sigma(u-1)^{a\sigma} - (z^\sigma - y^\sigma + 1)u^{a\sigma} - y^\sigma(u+1)^{a\sigma} + (u^2-1)^{a\sigma} = 0$$

and $x^{a\sigma} = x^{2-a}$ in $GF(3^{2n+1})^*$, hence it holds

$$z^\sigma(u-1)^2/(u-1)^a - (z^\sigma - y^\sigma + 1)u^2/u^a - y^\sigma(u+1)^2/(u+1)^a + (u^2-1)^2/(u^2-1)^a = 0.$$

Apply $\sigma$ again. And again. To see what you get, write

$$X = (u-1)^a, Y = u^a, Z = (u+1)^a,$$

so if $X$, $Y$, and $Z$ are not 0 one finds

$$\begin{cases} zX - (z-y+1)Y - yZ + XZ = 0, \\ z^\sigma(u-1)^2/X - (z^\sigma - y^\sigma + 1)u^2/Y - y^\sigma(u+1)^2/Z + (u^2-1)^2/XZ = 0, \\ z^{\sigma^2}(u-1)^{2\sigma-2}X - (z^{\sigma^2} - y^{\sigma^2} + 1)u^{2\sigma-2}Y \\ \qquad - y^{\sigma^2}(u+1)^{2\sigma-2}Z + (u^2-1),^{2\sigma-2}XZ = 0, \\ z^{\sigma^2}(u-1)^{2\sigma^2-2\sigma+2}/X - \cdots + (u^2-1)^{2\sigma^2-2\sigma+2}/XZ = 0. \end{cases}$$

After clearing denominators, consider this as a system of 4 equations for the 3 unknowns $X, Y, Z$. A compatibility condition must be satisfied: the *eliminant* of the system must vanish.

In order to compute it, J. J. Sylvester comes to our rescue (see, as I did, Salmon's Higher Algebra) with his dialytic method. The unpleasant result is that a certain $16 \times 16$ determinant has to vanish.

The next step is to look at the determinant. When something complicated $= 0$, do not try to write it as a sum. First, try to write it as a PRODUCT! Indeed one can factor out two pieces which are $2 \times 2$ determinants. Hence

$$(2 \times 2\,\text{det}) \cdot (2 \times 2\,\text{det}) \cdot (12 \times 12\,\text{det}) = 0;$$

look at these $2 \times 2$ pieces. By a little work, one shows

$$2 \times 2\,\text{det} = 0 \Rightarrow \underbrace{(u^2-1)^2 zy - \big(1 + zy + u(z+y)\big)(z-y+1)}_{\text{call this } F} u^2 = 0.$$

call $12 \times 12\,\text{det} = \Delta$ (do *not* try to compute it). We have shown:

*Thompson's condition* $\Rightarrow F\Delta = 0$.

$F\Delta$ is a rational function over $GF(3)$ in the variables

$$\begin{aligned} &z, y \\ &z^{\sigma}, y^{\sigma}, u \\ &z^{\sigma^2}, y^{\sigma^2}, u^{\sigma} \\ &z^{\sigma^3}, y^{\sigma^3}, u^{\sigma^2}. \end{aligned}$$

Substitute

$$\begin{aligned} u &= z^{\sigma+1} - y^{\sigma+1} \\ u^{\sigma} &= z^{\sigma^2+\sigma} - y^{\sigma^2+\sigma} \\ u^{\sigma^2} &= z^{\sigma^3+\sigma^2} - y^{\sigma^3+\sigma^2}, \end{aligned}$$

substitute

$$\begin{aligned} y^{\sigma} &= \frac{1 + z^{\sigma+2}}{y^2}, \\ y^{\sigma^2} &= \frac{1 + z^{\sigma^2+2\sigma}}{(1 + z^{\sigma+2})^2}\, y^4, \\ y^{\sigma^3} &= \frac{1 + z^{\sigma^3+2\sigma^2}}{(1 + z^{\sigma^2+2\sigma})^2} \quad \frac{(1 + z^{\sigma+2})^4}{y^8}, \end{aligned}$$

clear denominators, and get

$$R(z, z^{\sigma}, z^{\sigma^2}, z^{\sigma^3}; y) = 0$$

where $R(z_0, z_1, z_2, z_3; y_0)$ is a polynomial over $GF(3)$ with

$$\begin{aligned} \deg_{z_0} R &\leqq 119 \\ \deg_{z_1} R &\leqq 73 \\ \deg_{z_2} R &\leqq 38 \\ \deg_{z_3} R &= 12 \\ \deg_{y_0} R &\leqq 106. \end{aligned}$$

It is now plain that it is almost hopeless to calculate $R$ explicitly. This does not mean that you have to give up. So let us stop here and go to the next two questions.

↗ Can a computer do it? Maybe there is some simplification at the end.

↘ Do I really need to compute it?
What kind of information on $R$ do I need in order to know $\sigma$?

A good trick in mathematics means looking ahead and find first what you need for a proof, then prove exactly what you need and no more. Then the proof is complete.

So go boldly forward making one giant step. When we started, our initial program was to to eliminate $u$, $y$ and obtain a polynomial equation in $z, z^{\sigma}, z^{\sigma^2}$. However, what is the point of doing this? Do we really gain something?

**New problem.** *Let* $q = p^m$. *Let* $\sigma \in Aut\big(GF(q)\big)$. *Let* $H(z, z^{\sigma}, \ldots, z^{\sigma^k}) = 0$ *for all* $z \in GF(q)^*$, *where* $H(z_0, z_1, \ldots, z_k)$ *is a polynomial (not identically* 0*) in* $k+1$ *variables. What can we say about* $\sigma$ *?*

Let

$$H(z_0, \ldots, z_k) = \sum x_{\nu_0, \ldots, \nu_k} z_0^{\nu_0} \ldots z_k^{\nu_k}$$

so that

$$H(z, z^{\sigma}, \ldots, z^{\sigma^k}) = \sum x_{\nu_0, \ldots, \nu_k} z^{\nu_0 + \nu_1 \sigma + \cdots + \nu_k \sigma^k} = 0.$$

Let $z^*$ be a generator of $GF(q)^*$ and put $z = 1, z^*, (z^*)^2, (z^*)^3, \ldots, (z^*)^{\ell}, \ldots$

We get

$$\sum \left\{(z^*)^{\nu_0 + \nu_1 \sigma + \cdots + \nu_k \sigma^k}\right\}^{\ell} x_{\nu_0, \ldots, \nu_k} = 0$$

$\ell = 0, 1, 2, 3, \ldots$. Let us do this for $\ell = 0, 1, \ldots, N-1$ with

$$N = \#\text{ coeff. of } H.$$

Then we have a homogeneous linear system of $N$ equations in $N$ unknowns. Hence

$$\det\left(\{(z^*)^{\nu_0 + \nu_1 \sigma + \cdots + \nu_k \sigma^k}\}^{\ell}\right)_{\{\underline{\nu}; \ell\}} = 0.$$

This is a *Vandermonde determinant* (my favorite determinant!) which factorizes as

$$\prod_{\underline{\nu} \neq \underline{\nu}'} \left\{(z^*)^{\nu_0 + \nu_1 \sigma + \cdots + \nu_k \sigma^k} - (z^*)^{\nu_0' + \nu_1' \sigma + \cdots + \nu_k' \sigma^k}\right\}.$$

Since the determinant vanishes, some factor has to vanish, and we have obtained a great simplification without doing a gigantic calculation! Hence we have

$$(z^*)^{a_k \sigma^k + \cdots + a_1 \sigma + a_0} = 1$$

with the $a_j$ not all 0, and clearly

$$|a_j| \leqq \deg_{z_j} H.$$

This holds for $z^*$. Taking powers, it holds in $GF(q)^*$. Identify $\sigma$ with an integer. We have shown

$$a_k \sigma^k + \cdots + a_1 \sigma + a_0 \equiv 0 \pmod{q-1}.$$

On the other hand $\sigma = p^t, t \geqq 0$. Does this put restrictions on $\sigma$? YES.

**Example.** Suppose $H$ is known to the extent of having a bound

$$\deg_{z_j} H < p^d.$$

Say $\sigma = p^t$ and $0 \leqq t \leqq \frac{m}{k} - d$ where $q = p^m$. Then

$$\begin{aligned} &|a_k\sigma^k + \ldots + a_1\sigma + a_0| \\ &\leqq (p^d - 1)\left(p^{m-kd} + p^{m-(k-1)d} + \cdots + p^{m-2d} + p^{\frac{m}{k}-d} + 1\right) \\ &< p^m(p^{-d} + p^{-2d} + \cdots) + p^{\frac{m}{k}} + p^d < p^m - 1 = q - 1 \end{aligned}$$

if say $m > 2kd + d$. The left-hand side is $\equiv 0 \pmod{q-1}$ but less than $q-1$. Hence it must be equal to $0$. Now we have an equation for $\sigma$ (we may assume $a_0 \neq 0$):

$$a_k\sigma^k + \ldots + a_1\sigma + a_0 = 0.$$

This is very strong. For example, $\sigma = p^t$ divides $a_0$ (the congruence mod $q-1$ has become a congruence modulo a power of $p$)! However, $1 \leqq |a_0| < p^d$. Hence $0 \leqq t < d$ and the whole interval $d \leqq t \leqq \frac{m}{k} - d$ is excluded! Moreover, $d$ is the logarithm (in base $p$) of $\max_j \deg_{z_j} H$, thus $d$ is fairly small even if $H$ has very large degrees. What happens if $\sigma = p^t$ with $t > \frac{m}{k} - d$? Nothing new. The argument is identical, with $\sigma^h = p^{th}$ replaced by $p^{th \pmod m}$. If we clean up this carefully we emerge with the sharp result:

**Theorem 3.** *Let $H(z_0, \ldots, z_k)$ be a polynomial over $GF(q)$, not identically $0$, let*

$$\deg_{z_j} H < p^d, \quad \varphi = \textit{Frobenius}, \quad \sigma \in \operatorname{Aut} GF(q),$$

*and let $H(z, z^\sigma, z^{\sigma^2}, \ldots, z^{\sigma^k}) = 0$ on $GF(q)^*$.*

*Then one of $\sigma, \sigma^2, \ldots, \sigma^k$ equals one of $\varphi^{-d+1}, \varphi^{-d+2}, \ldots, 1, \varphi, \ldots, \varphi^{d-1}$.*

It follows that in our elimination game we have only to *keep track of degrees*, the actual expression which comes out of the elimination being totally irrelevant. *This we can do*!

We had

$$R\left(z, z^\sigma, z^{\sigma^2}, z^{\sigma^3}; y\right) = 0.$$

Let us apply $\sigma$ and use $y^\sigma = \dfrac{1 + z^{\sigma+2}}{y^2}$ to obtain

$$R\left(z^\sigma, z^{\sigma^2}, z^{\sigma^3}, z^{\sigma^4}; \frac{1 + z^{\sigma+2}}{y^2}\right) = 0$$

yielding a *new* relation

$$R_1(z, z^\sigma, z^{\sigma^2}, z^{\sigma^3}, z^{\sigma^4}; y) = 0.$$

Eliminating $y$ means: take a resultant of $R$ and $R_1$ with respect to $y$ and get

$$H(z, z^\sigma, z^{\sigma^2}, z^{\sigma^3}, z^{\sigma^4}) = 0.$$

(A polynomial with up to $2.295\ldots \times 10^{23}$ terms, but we have no need to write it down, we need only its *degree*.)

Apply the theorem. In our case, $\deg_{z_j} H < 47007 < 3^{10}$. Hence

$$\sigma \text{ or } \sigma^2 \text{ or } \sigma^3 \text{ or } \sigma^4 = 3^{-9} \text{ or } 3^{-8} \text{ or } \ldots \text{ or } 3^7 \text{ or } 3^8 \text{ or } 3^9$$

giving us 76 possibilities. *Getting close* ...

One difficulty: How to prove that $H$ is not identically 0 without computing it? Let's put this aside. How to reduce the 76 possibilities to only $\sigma^2 = 3$?

**Idea.** Take for example $\sigma^4 = 3$. We had

$$R(z, z^\sigma, z^{\sigma^2}, z^{\sigma^3}; y) = 0.$$

Now

$$y^{\sigma^3} = \frac{1 + z^{\sigma^3+2\sigma^2}}{(1 + z^{\sigma^2+2\sigma})^2} \frac{(1 + z^{\sigma+2})^4}{y^8}$$

thus

$$y^3 = y^{\sigma^4} = \frac{1 + z^{3+2\sigma^3}}{(1 + z^{\sigma^3+2\sigma^2})^2} \frac{(1 + z^{\sigma^2+2\sigma})^4}{(1 + z^{\sigma+2})^8} y^{16}$$

and

$$(1 + z^{3+2\sigma^3})(1 + z^{\sigma^2+2\sigma})^4 y^{13} - (1 + z^{\sigma^3+2\sigma^2})^2 (1 + z^{\sigma+2})^8 = 0.$$

This is a *new* relation. Eliminate $y$ and something like

$$K(z, z^\sigma, z^{\sigma^2}, z^{\sigma^3}) = 0$$

appears, use the Theorem 3 and get

$$\sigma \text{ or } \sigma^2 \text{ or } \sigma^3 = 3^{-7} \text{ or } 3^{-6} \text{ or } \ldots \text{ or } 3^6 \text{ or } 3^7.$$

Now $\sigma^4 = 3$ and $\sigma^m = 3^\mu$ with $m = 1$, 2 or 3 and $|\mu| \leqq 7$.

*If we eliminate $\sigma$ then a compatibility condition on $q$ appears.*

We get *identity* $= (\sigma^4)^m (\sigma^m)^{-4} = 3^{m-4\mu}$. Now $3^{m-4\mu} =$ *identity* $\Leftrightarrow$ $2n + 1 | m - 4\mu$ and $m - 4\mu \neq 0$. Also

$$|m - 4\mu| \leqq 3 + 4 \cdot 7 = 31.$$

Hence:

$$\sigma^4 = 3 \Rightarrow 2n + 1 \leqq 31, \text{ i.e. } q \leqq 3^{31}$$

**Question.** What happens to $\sigma^2 = 3$? Since it is a non-trivial solution, something special must occur here. Not all difficulties are over.

**One last difficulty.** How to prove that $K$ is not identically 0 without computing it? We need this, because once we control $H \neq 0$ and $K \neq 0$ we see that $2n+1$ is bounded. A little work shows that indeed $2n + 1 \leqq 83$.

In general we do not compute $H$ and $K$ directly but instead keep their expressions as products of determinants. Several entries in the determinants are 0 and the entries themselves are polynomials of relatively low degree. Then explicit calculations of the determinants, after specializing well-chosen variables to 0 or $\infty$, become doable.

**Fact 1.** $H$ is not identically 0 if we modify the construction. The idea:

$$H = 0 \Rightarrow R(z, \ldots, z^{\sigma^3}; y) \text{ and } R_1(z, \ldots, z^{\sigma^4}; y) \text{ have a common factor in } y.$$

Now this factor cannot contain $z^{\sigma^4}$. Hence we may specialize $z^{\sigma^4}$ to $\infty$ and see that this factor is a common factor of $R(z, \ldots, z^{\sigma^3}; y)$ and the coefficient of $z^{12\sigma^4}$ in $R_1(z, \ldots, z^{\sigma^4}; y)$. This coefficient can be determined explicitly and shown to factorize very well. This determines the possible factors. However,

$$\text{factors } = 0 \Rightarrow F = 0.$$

$F$ was a factor of $R$. Modifying $R_1$, we may assume that the unknown common factor is $F$. This we check directly. There is a little handwaving here but it is dealt with in the paper.[4]

**Fact 2.** $K$ is not identically 0 unless $\sigma^2 = 3$. Idea: the same as before. Now the second equation is explicit and *irreducible*.[5] To check that it does not divide $R$ we specialize $z, z^\sigma, \ldots$ to 0 (with some care, however). Then the specialized $R$ becomes computable. If $\sigma^2 = 3$, the second equation becomes $y - 1$ and (no surprise) it divides $R$, so the method for determining $\sigma$ stops here.

**Conclusion.** *If* $q > 3^{83}$, *then* $\sigma^2 = 3$. *If* $q \leqq 3^{83}$, *we have* 178 *pairs* $(q, \sigma)$ *to check.*

**Finally.** Now it is the right time for calculations! If $q \leqq 3^{83}$, use a computer. This was done independently by A. Odlyzko and D. Hunt.

---

[4] Indeed there was some handwaving requiring a minor addition, see the note at the end.

[5] This uses Bourbaki Algèbre Ch. V, §11, Ex 12, p. 178.

**Additional note (2015).** During my attempt to solve the problem I was in correspondence with Thompson and he enthusiastically encouraged me to persevere till the end when I communicated to him a short list of possibilities for $\sigma$. He also informed me that he had obtained earlier a result of a similar type but his list of possibilities was much too large for examining all possible cases.

The whole proof of the uniqueness of the groups of Ree type was, as part of the revision of the classification of finite simple groups, carefully redone and simplified by Enguehard.[6] It turned out that at the end of the argument for Fact 1 I claimed that the polynomial $G(z_0, z_1; y) = y^3 F^\sigma$ was irreducible, by means of a specialization argument (which I left to the reader). Gaps and errors sometimes are left to the reader to discover them! Well, I did not realize that the specialization I used allowed the possibility of a factor depending only on $z_0$. Actually, $z_0$ was such a factor. So $G$ was reducible. The correction in the argument consisted in replacing $G$ by $z_0^{-1}G$, which was irreducible. Since $z_0 \in GF(q)^*$, the factor $z_0$ was irrelevant and could be removed before doing the elimination of the variable $y$. The presence of the factor $z_0$ should not be surprising because $z = 0$ implies $(z, y, u) = (0, 1, -1)$, which satisfies the Thompson equation for all $\sigma$.

(*Reçu le 9 novembre 2015*)

Enrico Bombieri, School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540, USA

*e-mail:* eb@ias.edu



[6] Enguehard M. and T. Peterfalvi, Révision dans les groupes finis. Groupes du type de Lie de rang 1, *Astérisque* **142–143** (1986), 1–296.