WARING'S PROBLEM FOR ALGEBRAIC NUMBER FIELDS AND PRIMES OF THE FORM $(p^r - 1)/(p^d - 1)$

Dedicated to Hans Rademacher on the occasion of his seventieth birthday

BY

PAUL T. BATEMAN AND ROSEMARIE M. STEMMLER[1]

1. Introduction

Let K be an algebraic number field of finite degree n over the rationals, and let $J(K)$ be its ring of integers. If m is a positive integer greater than unity, let $J_m(K)$ be the additive group generated by the m^{th} powers of the elements of $J(K)$. Clearly $J_m(K)$ is a subring of $J(K)$. Needless to say, $J_m(K)$ is that subset of $J(K)$ in which Waring's problem for m^{th} powers is to be considered. The identity

$$m!\,x = \sum_{k=0}^{m-1}(-1)^{m-1-k}\binom{m-1}{k}\{(x+k)^m - k^m\}$$

shows that

$$m!\,J(K) \subset J_m(K) \subset J(K).$$

Hence $J_m(K)$ consists of certain of the residue classes of $J(K)$ modulo $m!\,J(K)$. Further $J_m(K)$ can be determined in a particular case by an examination of the quotient ring $J(K)/\{m!\,J(K)\}$. This determination can be rather complicated, especially when m is composite.

When m is a prime q, the situation is somewhat simpler than in the general case. In particular, it is easy to characterize those algebraic number fields K for which $J_q(K) = J(K)$. We shall do this in this paper. Examples of our main result are as follows: (A) $J_3(K) = J(K)$ unless either 3 is ramified[2] in $J(K)$ or 2 has in $J(K)$ a prime ideal factor of second degree, (B) $J_{11}(K) = J(K)$ unless 11 is ramified in $J(K)$, (C) $J_{31}(K) = J(K)$ unless either 31 is ramified in $J(K)$ or 2 has in $J(K)$ a prime ideal factor of fifth degree or 5 has in $J(K)$ a prime ideal factor of third degree. For most primes q the situation is analogous to that for $q = 11$, that is, we *usually* can say that $J_q(K) = J(K)$ if and only if q is not ramified in $J(K)$. This generalizes the familiar result [10] that $J_2(K) = J(K)$ if and only if 2 is not ramified in $J(K)$.

The primes for which complications occur are those special primes q ex-

Received April 24, 1961; received in revised form August 16, 1961.

[1] This work was supported by the Office of Naval Research.

[2] The phrase "q is ramified in $J(K)$" means that q is divisible by the square of some prime ideal in $J(K)$. By the so-called ramification theorem (see [6]) the condition that q is ramified in $J(K)$ is equivalent to the condition that q divides the discriminant of K. Accordingly our results could easily be modified by replacing the former condition by the latter.

pressible in the form

$$(*) \qquad q = (p^r - 1)/(p^d - 1),$$

where p is also a prime number and r and d are positive integers. Here d must be a divisor of r, since otherwise $(p^r - 1)/(p^d - 1)$ would not be an integer, in view of the identity

$$(p^r - 1)/(p^d - 1) = \sum_{i=1}^{[r/d]} p^{r-id} + (p^{r-[r/d]d} - 1)/(p^d - 1),$$

where $[u]$ denotes the greatest integer not exceeding the real number u. Further r must actually be a prime-power, and d must be the largest divisor of r other than r itself, since otherwise $(p^r - 1)/(p^d - 1)$ would be composite, in view of the identity

$$(p^r - 1)/(p^d - 1) = \prod \Phi_j(p),$$

where j runs over the divisors of r which are *not* divisors of d, and $\Phi_j(x)$ is the j^{th} cyclotomic polynomial. Thus in specifying an expression for a prime q in the form $(*)$, it is enough to give the value of r.

Our precise result is the following, which is a restatement of Theorem 3 below. *If q is a prime number not expressible in the form $(*)$, then $J_q(K) = J(K)$ if and only if q is unramified in $J(K)$. If q is a prime number expressible in the form $(*)$, let*

$$q = (p_1^{r_1} - 1)/(p_1^{d_1} - 1), \quad \cdots, \quad q = (p_v^{r_v} - 1)/(p_v^{d_v} - 1)$$

be all the ways it can be so expressed. Then $J_q(K) = J(K)$ if and only if q is unramified in $J(K)$ and p_i does not have in $J(K)$ a prime ideal factor of degree r_i for $i = 1, 2, \cdots, v$.

The prime numbers of the form $(*)$ are comparatively rare. For example, the table at the end of the paper shows that there are only 28 of them less than $(10)^5$. Within the range of the table, 31 is the only prime with more than one expression in the form $(*)$. We shall show by the sieve method that $\sum^* q^{-1/2}$ converges, where the sum runs over the primes of the form $(*)$, each taken in the multiplicity of its occurrence in the form $(*)$. More specifically, we shall show that if x is large, there are at most $50\, x^{1/2}(\log x)^{-2}$ primes of the form $(*)$ not exceeding x, repetitions counting.

Special cases of our main result such as (A), (B), and (C) above can easily be read off by use of the table.

Siegel [9, 10] has shown that if ν is a totally positive element of $J_m(K)$, then ν is expressible as a sum of $(2^{m-1} + n)mn + 1$ or fewer m^{th} powers of totally positive elements of $J(K)$, provided that, if K is totally real, the norm of ν is sufficiently large. Tatuzawa [12] has improved this result by showing that $8mn(m + n)$ or fewer summands will suffice.[3] It would naturally be desirable to eliminate the strong dependence of these results on the

[3] A further improvement was obtained recently by O. KÖRNER, *Über das Waringsche Problem in algebraischen Zahlkörper*, Math. Ann., vol. 144 (1961), pp. 224–238.

field degree n. While this would probably be a rather ambitious task, on the other hand one of us has shown that a result of this kind is readily obtainable for the so-called easier Waring problem. Specifically, it is shown in [11] that for any prime q every element ν of $J_q(K)$ is expressible as a sum of at most $2^{q-1} + q/3 + 1$ integers of the form $\pm\lambda^q$, where $\lambda \in J(K)$. The results obtained in this paper tell us for which fields K we can make such an assertion for every element ν of $J(K)$.

2. A theorem of Tornheim

We shall require the following result of Tornheim [13] and so we include a brief proof for convenience. As is customary we denote the finite field of p^r elements, where p is a prime, by $GF(p^r)$.

THEOREM 1. *Suppose q is a prime. Then every element of $GF(p^r)$ is expressible as a sum of q^{th} powers of elements of $GF(p^r)$ unless $q = (p^r - 1)/(p^d - 1)$ for some divisor d of r, in which special case the q^{th} powers form a subfield of p^d elements.*

Proof. If $q \nmid (p^r - 1)$, then the operation of taking the q^{th} power gives an automorphism of the multiplicative group of $GF(p^r)$, and hence every element of $GF(p^r)$ is a q^{th} power. If $q \mid (p^r - 1)$, regardless of whether or not q has the special form mentioned in the statement of the theorem, the nonzero q^{th} powers form a subgroup H of index q in the multiplicative group of $GF(p^r)$. If $q = (p^r - 1)/(p^d - 1)$ for some divisor d of r, then H must coincide with the multiplicative group of that subfield of $GF(p^r)$ which has p^d elements, so that in this case we have the result indicated. Now suppose $q \mid (p^r - 1)$ but q does not have the previous special form. Then H does not coincide with the multiplicative group of any subfield of $GF(p^r)$. However, the set L consisting of those elements of $GF(p^r)$ which are expressible as the sum of q^{th} powers is closed under addition and multiplication, and therefore L is a subfield of $GF(p^r)$. Thus the multiplicative group of L properly contains H. Since H has prime index q in the multiplicative group of $GF(p^r)$, we must have $L = GF(p^r)$. This completes the proof.

3. How to determine $J_q(K)$

The Chinese Remainder Theorem enables us to prove the following result on the determination of $J_q(K)$, which is implicit in [11].

THEOREM 2. *Suppose q is a prime number. Suppose $P_1, P_2, \cdots, P_s$ are the distinct prime ideals of $J(K)$ dividing $(q-1)!$. Then an element ν of $J(K)$ is in $J_q(K)$ if and only if it satisfies the following conditions:*

(a) *For each i $(i = 1, 2, \cdots, s)$ there are elements $\rho_{i1}, \cdots, \rho_{im(i)}$ of $J(K)$ such that*

$$\nu \equiv \rho_{i1}^{\,q} + \cdots + \rho_{im(i)}^{\,q} \pmod{P_i}.$$

(b) *There is an element δ of $J(K)$ such that*

$$\nu \equiv \delta^q \pmod{qJ(K)}.$$

Remark. In order to obtain the result on the easier Waring problem mentioned at the end of §1, all we need do, in view of the identity of the first paragraph of §1, is to show that we can always take $m(i) \leqq q/3$. This is rather simple to do by easy group-theoretic arguments.

Proof. First suppose $\nu \in J_q(K)$. Then by definition ν is the sum of a finite number of elements of the form $\pm\lambda^q$, where $\lambda \in J(K)$. Since

$$-\lambda^q \equiv (-\lambda)^q \pmod{q!\, J(K)},$$

this implies that ν is congruent to a sum of q^{th} powers modulo $q!\, J(K)$. Hence (a) holds. Since

$$\mu_1^q + \mu_2^q + \cdots + \mu_n^q \equiv (\mu_1 + \mu_2 + \cdots + \mu_n)^q \pmod{qJ(K)},$$

for any $\mu_1, \mu_2, \cdots, \mu_n$ in $J(K)$, it follows that (b) holds also.

Now suppose (a) and (b) hold. By inserting zero terms if necessary we may assume that $m_1, m_2, \cdots, m_s$ all have the same value $m - 1$. For $j = 1, \cdots, m - 1$ we choose $\gamma_j \in J(K)$ by the Chinese Remainder Theorem so that

$$\gamma_j \equiv \rho_{ij} \pmod{P_i} \qquad (i = 1, \cdots, s).$$

Put $\gamma_m = -1$. Then

$$\nu \equiv 1^q + \gamma_1^q + \cdots + \gamma_m^q \pmod{P_1 P_2 \cdots P_s}.$$

Define a sequence $\beta_1, \beta_2, \cdots$ of elements of $J(K)$ as follows. Put $\beta_1 = 1$ and

$$\beta_{k+1} = \beta_k + h(\nu - \beta_k^q - \gamma_1^q - \cdots - \gamma_m^q),$$

where h is a fixed rational integer such that $hq \equiv 1 \pmod{(q-1)!}$. Then it is easy to see by induction that $\beta_k \equiv 1 \pmod{P_1 P_2 \cdots P_s}$ and

$$\nu \equiv \beta_k^q + \gamma_1^q + \cdots + \gamma_m^q \pmod{(P_1 P_2 \cdots P_s)^k}$$

for any positive integral value of k. Choose k so large that

$$(q - 1)!\, J(K) \mid (P_1 P_2 \cdots P_s)^k.$$

Choose α_0 in $J(K)$ so that for this value of k we have

$$\alpha_0 \equiv \beta_k \pmod{(q-1)!\, J(K)}, \qquad \alpha_0 \equiv \delta \pmod{qJ(K)},$$

and for $j = 1, 2, \cdots, m$ choose α_j in $J(K)$ so that

$$\alpha_j \equiv \gamma_j \pmod{(q-1)!\, J(K)}, \qquad \alpha_j \equiv 0 \pmod{qJ(K)}.$$

Then clearly

$$\nu \equiv \alpha_0^q + \alpha_1^q + \cdots + \alpha_m^q \pmod{q!\, J(K)},$$

since this congruence holds both modulo $(q - 1)!\, J(K)$ and modulo $qJ(K)$.

Since $q!\,J(K) \subset J_q(K)$, we conclude that $\nu \in J_q(K)$. Hence (a) and (b) imply that $\nu \in J_q(K)$.

4. Main result on the characterization of $J_q(K)$

The previous two theorems enable us to prove the following main result.

THEOREM 3. *Suppose q is a prime number. Then $J_q(K) \neq J(K)$ if and only if at least one of the following holds:*

(i) *q is ramified in $J(K)$.*

(ii) *q is expressible in the form $(p^r - 1)/(p^d - 1)$, where p is a prime and r and d are positive integers, and p has in $J(K)$ a prime ideal factor of degree r.*

Proof. Suppose (i) holds. Then $qJ(K)$ is divisible by the square of some prime ideal Q in $J(K)$. Thus the coprime-residue-class group modulo $qJ(K)$ has order divisible by q. Hence not all coprime-residue-classes contain q^{th} powers, since in an Abelian group of order divisible by q the mapping $X \to X^q$ is a homomorphism of the group strictly into itself. Therefore, by Theorem 2, $J_q(K)$ is properly contained in $J(K)$ when (i) holds.

Suppose (ii) holds. Suppose P is a prime ideal in $J(K)$ of degree r which divides p. Then $GF(NP)$ falls under the exceptional case of Theorem 1. Thus by Theorem 1 not all residue-classes modulo P contain sums of q^{th} powers. Therefore by Theorem 2, $J_q(K)$ is properly contained in $J(K)$ when (ii) holds.

Now suppose neither (i) nor (ii) holds. Suppose $P_1, P_2, \cdots, P_s$ are the distinct prime ideals dividing $(q-1)!\,J(K)$. Since (ii) does not hold, for $i = 1, 2, \cdots, s$ we know that $GF(NP_i)$ does not come under the exceptional case of Theorem 1. It follows that for $i = 1, 2, \cdots, s$ every residue-class modulo P_i contains a sum of q^{th} powers. Thus condition (a) of Theorem 2 holds for any ν in $J(K)$. On the other hand, since (i) does not hold,

$$qJ(K) = Q_1 Q_2 \cdots Q_t,$$

where $Q_1, Q_2, \cdots, Q_t$ are distinct prime ideals. If $\nu \in J(K)$ and if we choose $\delta \in J(K)$ so that

$$\delta \equiv \nu^{NQ_j/q} \pmod{Q_j} \qquad (j = 1, \cdots, t),$$

we will have

$$\delta^q \equiv \nu^{NQ_j} \equiv \nu \pmod{Q_j} \qquad (j = 1, \cdots, t),$$

and thus

$$\delta^q \equiv \nu \pmod{qJ(K)}.$$

Thus condition (b) of Theorem 2 holds for any ν in $J(K)$. Since conditions (a) and (b) of Theorem 2 hold for any ν in $J(K)$, it follows that $J_q(K) = J(K)$ when neither (i) nor (ii) holds. Thus Theorem 3 is proved.

As mentioned in the Introduction, the exceptional case of Theorem 1 and the case (ii) of Theorem 3 cannot occur unless r is a prime-power and d is the largest divisor of r other than r itself.

Our arguments enable us to give the following description of $J_q(K)$ when

$J_q(K) \neq J(K)$. If (i) holds but (ii) does not, then $J_q(K)$ is equal to the ring $R_q(K)$ consisting of those integers of K which are congruent to q^{th} powers modulo $qJ(K)$. If (ii) holds but (i) does not, then $J_q(K)$ is equal to the ring $S_q(K)$ consisting of those integers of K which are congruent to q^{th} powers modulo each of the prime ideals of the type referred to in the statement of (ii). If both (i) and (ii) hold, then $J_q(K) = R_q(K) \cap S_q(K)$.

5. Frequency of occurrence of primes of the form (*)

Let $H(x)$ denote the number of primes q not exceeding x and expressible in the form (*) for some prime p and some positive integers[4] r and d, each q being counted according to the multiplicity of its occurrence in the form (*). (Thus 31 is counted twice.) In this section we use Atle Selberg's sieve method to show that $H(x) \leqq 50\, x^{1/2}(\log x)^{-2}$ for large x. The crude form of Brun's sieve method given in [5] would show that

$$H(x) = O(x^{1/2}(\log \log x)^2\, (\log x)^{-2})$$

for large x, which would be sufficient to show that $\sum^* q^{-1/2}$ converges. Our proof will be accomplished by means of several lemmas. In what follows, sums or products on the letter p are to be extended over the primes, and sums on the letter m are to be extended over the positive integers.

LEMMA 1 (Atle Selberg). *Suppose F is a polynomial in one variable with integral coefficients. Suppose N is a positive integer greater than* 1 *and* $1 < z < N$. *Let S be the number of positive integers j between* 1 *and N inclusive such that $F(j)$ is relatively prime to $\prod_{p \leqq z} p$. Let $\omega(m)$ denote the number of solutions of the congruence*

$$F(X) \equiv 0 \pmod{m}.$$

If $\omega(p) = p$ for some prime p not exceeding z, then $S = 0$. If $\omega(p) < p$ for all primes p not exceeding z, then

$$S \leqq N/Z + R,$$

where

$$Z = \sum\nolimits_{m \leqq z} a_m\, m^{-1}, \qquad a_m = \mu^2(m)\omega(m) \prod\nolimits_{p \mid m} (1 - \omega(p)/p)^{-1},$$

$$R = z^2 \prod\nolimits_{p \leqq z} (1 - \omega(p)/p)^{-2}.$$

Proof. See [8].

LEMMA 2. *Suppose F is the product of k distinct polynomials with integral coefficients each irreducible over the field of rational numbers. Suppose $\omega(m)$ and a_m are defined as in Lemma* 1. *If $\omega(p) < p$ for all primes p, then for x large*

$$\sum\nolimits_{m \leqq x} a_m\, m^{-1} = \{k!\, C(F)\}^{-1}(\log x)^k + A_{k-1}(\log x)^{k-1} + \cdots + A_1 \log x + A_0 + O(x^{\theta - 1}),$$

[4] In view of the remarks made in the introduction, r must actually be a prime-power, and d must be the largest divisor of r other than r itself.

where $A_0, \cdots, A_{k-1}$ *are certain constants depending on* F,

$$C(F) = \prod_p \{(1 - 1/p)^{-k}(1 - \omega(p)/p)\},$$

and θ *is a number between* $\frac{1}{2}$ *and* 1 *depending only on the degrees of the factors of* F.

Proof. Suppose the k irreducible factors of F are $f_1, f_2, \cdots, f_k$, and let $\omega_i(m)$ be the number of solutions of the congruence $f_i(X) \equiv 0 \pmod{m}$. Then for all but finitely many primes p we know that $\omega_i(p)$ is the number of distinct prime ideals of first degree in the algebraic number field generated by a zero of f_i (see [16]). It is also known that

$$\sum_p (\omega_i(p) - 1)/p$$

converges. Clearly $\omega(p) = \omega_1(p) + \cdots + \omega_k(p)$ for all but finitely many primes p, so that

$$\sum_p (\omega(p) - k)/p$$

converges. Then for Re $s > 1$ we have

$$\begin{aligned}\sum_m \frac{a_m}{m^s} &= \prod_p \left\{1 + \frac{\omega(p)}{p^s}\left(1 - \frac{\omega(p)}{p}\right)^{-1}\right\} \\ &= \sum_m \frac{\delta_m}{m^s} \cdot \prod_p \left(1 - \frac{\omega(p)}{p^s}\right)^{-1} \\ &= \sum_m \frac{\varepsilon_m}{m^s} \cdot \prod_p \left(1 - \frac{\omega_1(p) + \cdots + \omega_k(p)}{p^s}\right)^{-1} \\ &= \sum_m \frac{\eta_m}{m^s} \cdot \prod_p \left\{\left(1 - \frac{\omega_1(p)}{p^s}\right) \cdots \left(1 - \frac{\omega_k(p)}{p^s}\right)\right\}^{-1} \\ &= \sum_m \frac{\theta_m}{m^s} \cdot \zeta_1(s) \cdots \zeta_k(s),\end{aligned}$$

where $\zeta_i(s)$ is the Dedekind zeta-function of the field generated by a zero of f_i, and $\sum \delta_m m^{-s}$, $\sum \varepsilon_m m^{-s}$, $\sum \eta_m m^{-s}$, and $\sum \theta_m m^{-s}$ converge absolutely for Re $s > \frac{1}{2}$. Now put (for Re $s > 1$)

$$\sum b_m m^{-s} = \zeta_1(s) \cdots \zeta_k(s).$$

Then by an elementary argument of the type discussed in [14] we readily deduce from Weber's theorem [15, 16] that

$$\sum_{m \leqq x} b_m = B_{k-1}\, x(\log x)^{k-1} + B_{k-2}\, x(\log x)^{k-2} + \cdots + B_0\, x + O(x^\theta),$$

where θ is as announced. (Complex-variable methods using the functional equation of the Dedekind zeta-function would give a better value of θ.) A further elementary argument gives as an immediate consequence of the above

$$\sum_{m \leqq x} a_m = D_{k-1}\, x(\log x)^{k-1} + D_{k-2}\, x(\log x)^{k-2} + \cdots + D_0\, x + O(x^\theta),$$

where $D_0, D_1, \cdots, D_{k-1}$ are certain constants. But

$$\begin{aligned}(k-1)!\,D_{k-1} &= \lim_{s\to 1+} (s-1)^k \sum_m a_m m^{-s} \\ &= \lim_{s\to 1+} \zeta(s)^{-k} \sum_m a_m m^{-s} \\ &= \lim_{s\to 1+} \prod_p \left\{\left(1-\frac{1}{p^s}\right)^k\left(1+\frac{\omega(p)(1-\omega(p)/p)^{-1}}{p^s}\right)\right\} \\ &= \prod_p \left\{\left(1-\frac{1}{p}\right)^k\left(1+\frac{\omega(p)}{p-\omega(p)}\right)\right\} = \frac{1}{C(F)},\end{aligned}$$

where the limit step follows from the fact that

$$\lim_{s\to 1+} \sum_p \frac{\omega(p)-k}{p^s} = \sum_p \frac{\omega(p)-k}{p}.$$

The result of the lemma now follows from the formula

$$\sum_{m\leqq x} a_m m^{-1} = x^{-1}\sum_{m\leqq x} a_m + \int_1^x u^{-2}\left(\sum_{m\leqq u} a_m\right) du.$$

LEMMA 3. *Suppose $f_1, f_2, \cdots, f_k$ are distinct irreducible polynomials with integral coefficients and positive leading coefficients, and suppose F is their product. Let $Q_F(N)$ be the number of positive integers j between 1 and N inclusive such that $f_1(j), \cdots, f_k(j)$ are all primes. Then for large N we have*

$$Q_F(N) \leqq 2^k k!\, C(F) N(\log N)^{-k} + o(N(\log N)^{-k}).$$

Remark. Heuristically we would expect to have

$$Q_F(N) = h_1^{-1}h_2^{-1}\cdots h_k^{-1} C(F)\int_2^N (\log u)^{-k}\,du + o(N(\log N)^{-k}),$$

where $h_1, h_2, \cdots, h_k$ are the degrees of $f_1, f_2, \cdots, f_k$ respectively. Thus Selberg's method gives an upper bound for $Q_F(N)$ which is $2^k k!\, h_1 h_2 \cdots h_k$ times the conjectured asymptotic value.

Proof. The result is trivial if $\omega(p) = p$ for some prime p. Otherwise we apply Lemma 1 to F with $z = N^{1/2}(\log N)^{-(3k+1)/2}$. In view of Lemma 2 the quantity Z of Lemma 1 satisfies

$$Z = \{k!\,C(F)\}^{-1}\{\log z\}^k + O(\{\log z\}^{k-1}).$$

Also

$$\begin{aligned}R &= z^2 \exp\{-2 \textstyle\sum_{p\leqq z} \log(1-\omega(p)p^{-1})\} \\ &= z^2 \exp\{2 \textstyle\sum_{p\leqq z} (kp^{-1} + c_p - d_p)\},\end{aligned}$$

where

$$c_p = \frac{\omega(p)-k}{p}, \qquad d_p = \frac{\omega(p)}{p} + \log\left(1-\frac{\omega(p)}{p}\right).$$

Since $\sum c_p$ and $\sum d_p$ converge and since

$$\sum_{p\leqq z} p^{-1} = \log\log z + O(1),$$

we have

$$R \leqq z^2 \exp\,(2k \log\log z + \log B) = Bz^2(\log z)^{2k},$$

where B is a positive constant. Thus

$$\begin{aligned} Q_F(N) &\leqq O(z) + S \\ &\leqq O(z) + N/Z + R \\ &= O(z) + k!\, C(F)N(\log z)^{-k} + O(N(\log z)^{-k-1}) + O(z^2(\log z)^{2k}). \end{aligned}$$

In view of our choice of z we have

$$Q_F(N) \leqq 2^k k!\, C(F)N(\log N)^{-k} + O(N(\log\log N)(\log N)^{-k-1}),$$

which gives the result of Lemma 3.

LEMMA 4. *Suppose r is a prime-power and d is the largest divisor of r other than r itself. Let $P_r(N)$ denote the number of primes p such that $p \leqq N$ and $(p^r - 1)/(p^d - 1)$ is prime. If r is a power of 2, then $P_r(N) \leqq 1$. If r is a power of an odd prime, then for large N we have*

$$P_r(N) \leqq 8C_r N(\log N)^{-2} + o(N(\log N)^{-2}).$$

Here

$$C_r = \prod_p \{(1 - 1/p)^{-2}(1 - \omega(p)/p)\},$$

where $\omega(p) = 2$ if $p \mid r$, $\omega(p) = \phi(r) + 1$ if $p \equiv 1 \pmod r$, and $\omega(p) = 1$ otherwise.

Remark. Heuristically we would expect to have

$$P_r(N) \sim r^{-1}C_r \int_2^N (\log u)^{-2}\, du$$

as $N \to +\infty$. Also note that

$$\omega(p) = 2 + \chi_1(p) + \cdots + \chi_{\phi(r)-1}(p),$$

where $\chi_1, \cdots, \chi_{\phi(r)-1}$ are the nonprincipal residue-characters modulo r.

Proof. If r is a power of 2, then

$$(p^r - 1)/(p^d - 1) = p^d + 1,$$

which is divisible by 2 when p is odd. Thus $P_r(N) \leqq 1$, with equality only if $2^d + 1$ is a Fermat prime and $N \geqq 2$. Now suppose r is a power of an odd prime. Then, in view of Lemma 3, all we need to do is find the number $\omega(p)$ of solutions of the congruence

$$X(X^{r-d} + X^{r-2d} + \cdots + X^d + 1) \equiv 0 \pmod p, \tag{1}$$

which is one more than the number of solutions of the congruence

$$(2)\qquad X^{r-d} + X^{r-2d} + \cdots + X^{d} + 1 \equiv 0 \pmod{p}.$$

Any solution of (2) is relatively prime to p and satisfies $X^r \equiv 1 \pmod{p}$, so that its multiplicative order modulo p must be a divisor of r. But if the multiplicative order of X_0 is a divisor of r other than r itself, then $X_0^{\,d} \equiv 1 \pmod{p}$, and so

$$r/d \equiv X_0^{\,r-d} + X_0^{\,r-2d} + \cdots + 1 \equiv 0 \pmod{p}.$$

Thus if p does not divide r, the number of solutions of (2) is equal to the number of elements of exact order r in the coprime-residue-class group modulo p, namely, $\phi(r)$ if $p \equiv 1 \pmod{r}$ and zero if $p \not\equiv 1 \pmod{r}$. If p is the unique prime dividing r, then $X \equiv 1 \pmod{p}$ is a solution of (2) and is the only one, since no other element of the coprime-residue-class group modulo p has order dividing r. Thus the number of solutions of (1) is as given in the statement of the lemma.

LEMMA 5. *Let $P_3(N)$ denote the number of primes p such that $p \leqq N$ and $p^2 + p + 1$ is prime. Then for large N we have*

$$P_3(N) \leqq 8C_3 N(\log N)^{-2} + o(N(\log N)^{-2}),$$

where

$$C_3 = \prod_p \left\{\left(1 - \frac{1}{p}\right)^{-2}\left(1 - \frac{2 + \chi(p)}{p}\right)\right\} = 1.52\cdots$$

and $\chi(p) = -1, 0,$ or 1 according as p is congruent to $-1, 0,$ or 1 modulo 3. In particular

$$P_3(N) \leqq 12.3\, N(\log N)^{-2}$$

for all sufficiently large N.

Remark. The heuristic result here is

$$P_3(N) \sim \tfrac{1}{2}\, C_3 \int_2^N (\log u)^{-2}\, du = 0.76\cdots \int_2^N (\log u)^{-2}\, du$$

as $N \to +\infty$. We notice that

$$\begin{aligned} C_3 &= L(1, \chi)^{-1} \prod_p \left\{\left(1 - \frac{1}{p}\right)^{-2}\left(1 - \frac{\chi(p)}{p}\right)^{-1}\left(1 - \frac{2 + \chi(p)}{p}\right)\right\} \\ &= \frac{3\sqrt{3}}{\pi} \prod_p \left\{\left(\frac{p}{p-1}\right)^{2}\left(\frac{p - \chi(p) - 2}{p - \chi(p)}\right)\right\} \\ &= 1.6539\cdots \prod_p \left\{1 - \frac{p + 2\chi(p)p - \chi(p)}{(p-1)^2(p - \chi(p))}\right\}. \end{aligned}$$

Proof. Lemma 5 is a special case of Lemma 4.

LEMMA 6. *Suppose $H(x)$ is defined as at the beginning of this section and $P_3(x)$ is as defined in Lemma 5. Then*

$$H(x) = P_3(x^{1/2}) + O(x^{1/4}(\log x)^{-2}).$$

Proof. If r is a fixed prime-power and d is the largest divisor of r other than r itself, let $G_r(x)$ denote the number of primes q such that $q \leqq x$ and $q = (p^r - 1)/(p^d - 1)$ for some prime p. Since

$$(p^r - 1)/(p^d - 1) \geqq p^{r-d} \geqq 2^{r-d} \geqq 2^{r/2} \geqq e^{r/3},$$

we have

$$H(x) = \sum\nolimits_{r \leqq 3\log x} G_r(x).$$

Since $p^2 + p + 1 \leqq x$ if and only if $p \leqq (x - \frac{3}{4})^{1/2} - \frac{1}{2}$, we have

$$G_3(x) = P_3((x - \tfrac{3}{4})^{1/2} - \tfrac{1}{2}) = P_3(x^{1/2}) + O(1).$$

By Lemma 4

$$G_5(x) \leqq P_5(x^{1/4}) = O(x^{1/4}(\log x)^{-2}).$$

If r is an odd prime-power greater than 6, we have trivially

$$G_r(x) \leqq x^{1/(r-d)} = x^{1/\phi(r)} \leqq x^{1/6}.$$

Finally if r is a power of 2, then

$$G_r(x) \leqq 1 \leqq x^{1/6}.$$

Combining these results, we have

$$\begin{aligned} H(x) &= P_3(x^{1/2}) + O(1) + O(x^{1/4}(\log x)^{-2}) + O(x^{1/6} \log x) \\ &= P_3(x^{1/2}) + O(x^{1/4}(\log x)^{-2}). \end{aligned}$$

THEOREM 4. *If $H(x)$ denotes the number of primes of the form $(*)$ not exceeding x, then*

$$H(x) \leqq 50\, x^{1/2}(\log x)^{-2} \leqq 12.5 \int_2^{x^{1/2}} (\log u)^{-2}\, du$$

for all sufficiently large x.

Remark. Heuristically we would expect to have (as $x \to +\infty$)

$$H(x) \sim P_3(x^{1/2}) \sim \tfrac{1}{2}C_3 \int_2^{x^{1/2}} (\log u)^{-2}\, du = 0.76\cdots \int_2^{x^{1/2}} (\log u)^{-2}\, du.$$

Proof. The theorem follows from Lemmas 5 and 6.

COROLLARY. *The series $\sum^* q^{-1/2}$ converges, the sum being taken over all primes of the form $(*)$, each taken in the multiplicity of its occurrence in the form $(*)$.*

Proof. Cf. the proof of Theorem 120 of [5].

6. Numerical data

Table II lists the first 240 primes q of the form

$$(*) \qquad q = (p^r - 1)/(p^d - 1),$$

where p is a prime and r and d are positive integers. It is part of a more extensive unpublished table giving the 814 such primes less than 1.275×10^{10}.

Most primes of the form $(*)$ have $r = 3$, that is, are of the form $p^2 + p + 1$, where p is a prime. In fact up to 1.275×10^{10} there are only 38 primes of the form $(*)$ with $r \neq 3$; these are already known and can be found among the data in [1], [2], and [3]. However, Table II apparently does go beyond previously published tables of primes of the form $p^2 + p + 1$. This was made possible by the efforts of Mr. Roger A. Horn, a student in the 1961 Undergraduate Summer Program of the University of Illinois Digital Computer Laboratory, who used the Illiac to prepare a list of the 776 primes of the form $p^2 + p + 1$ less than 1.275×10^{10}. Up to 1.21×10^8 Mr. Horn's list agrees perfectly with a similar but shorter list made earlier by us from inspection of Poletti's table [7] of the primes of the form $N^2 + N + 1$ less than 1.21×10^8, except that we had missed 86927653 because of a typographical error in Poletti's paper. (Poletti's list gives 86927653 as $(9333)^2 + 9333 + 1$ instead of as $(9323)^2 + 9323 + 1$.)

The 38 primes of the form $(*)$ which do not exceed 1.275×10^{10} and which have $r \neq 3$ are distributed as follows: sixteen are of the form $(p^5 - 1)/(p - 1)$, six are of the form $(p^7 - 1)/(p - 1)$, three are of the form $(p^9 - 1)/(p^3 - 1)$, three are of the form $(p^{13} - 1)/(p - 1)$, and there are ten primes which are one of a kind, namely $2^1 + 1$, $2^2 + 1$, $2^4 + 1$, $2^8 + 1$, $2^{16} + 1$, $2^{17} - 1$, $2^{18} + 2^9 + 1$, $2^{19} - 1$, $(5^{11} - 1)/(5 - 1)$, and $2^{31} - 1$.

Table I shows that the numerical data agree remarkably well with the heuristic formulas mentioned in the remarks after Lemma 5 and Theorem 4.

TABLE I

x	$H(x)$	$G_3(x)$	$\frac{1}{2}C_3 \int_2^{x^{1/2}} (\log u)^{-2}\, du$
10^1	3	1	1
10^2	8	3	3
10^3	12	4	5
10^4	19	8	8
10^5	28	13	14
10^6	44	23	26
10^7	76	52	55
10^8	146	117	123
10^9	318	286	292
10^{10}	744	706	720
1.275×10^{10}	814	776	793

TABLE II

Table of primes q of the form $q = (p^r - 1)/(p^d - 1)$, where p is a prime and r and d are positive integers.

q	p^r	q	p^r	q	p^r
3	2^2	732 541	29^5	12 190 573	3491^3
5	2^4	735 307	857^3	12 207 031	5^{11}
7	2^3	797 161	3^{13}	12 655 807	3557^3
13	3^3	830 833	911^3	13 479 913	3671^3
17	2^8	1 191 373	1091^3	15 066 043	3881^3
31	2^5	1 204 507	1097^3	15 916 111	3989^3
31	5^3	1 353 733	1163^3	17 284 807	4157^3
73	2^9	1 395 943	1181^3	17 787 307	4217^3
127	2^7	1 424 443	1193^3	18 143 341	4259^3
257	2^{16}	1 482 307	1217^3	19 443 691	4409^3
307	17^3	1 772 893	11^9	22 292 563	4721^3
757	3^9	1 886 503	1373^3	22 406 023	4733^3
1 093	3^7	2 037 757	1427^3	22 576 753	4751^3
1 723	41^3	2 212 657	1487^3	23 790 007	4877^3
2 801	7^5	2 432 041	1559^3	23 907 211	4889^3
3 541	59^3	2 507 473	1583^3	24 735 703	4973^3
5 113	71^3	2 922 391	1709^3	25 035 013	5003^3
8 011	89^3	3 281 533	1811^3	25 396 561	5039^3
8 191	2^{13}	3 413 257	1847^3	25 646 167	17^7
10 303	101^3	3 500 201	43^5	25 882 657	5087^3
17 293	131^3	3 730 693	1931^3	28 638 553	5351^3
19 531	5^7	3 894 703	1973^3	28 792 661	73^5
28 057	167^3	4 534 771	2129^3	30 266 503	5501^3
30 103	173^3	5 168 803	2273^3	34 427 557	5867^3
30 941	13^5	5 229 043	13^7	36 572 257	6047^3
65 537	2^{32}	5 333 791	2309^3	38 112 103	6173^3
86 143	293^3	5 473 261	2339^3	39 449 441	79^5
88 741	17^5	5 815 333	2411^3	40 825 711	6389^3
131 071	2^{17}	7 094 233	2663^3	42 922 153	6551^3
147 073	383^3	7 450 171	2729^3	43 158 331	6569^3
262 657	2^{27}	7 781 311	2789^3	43 553 401	6599^3
292 561	23^5	8 746 807	2957^3	44 269 063	6653^3
459 007	677^3	8 817 931	2969^3	45 151 681	6719^3
492 103	701^3	9 069 133	3011^3	45 717 883	6761^3
524 287	2^{19}	9 250 723	3041^3	46 124 473	6791^3
552 793	743^3	9 843 907	3137^3	46 696 723	6833^3
579 883	761^3	10 378 063	3221^3	47 851 807	6917^3
598 303	773^3	10 572 253	3251^3	48 037 081	83^5
684 757	827^3	11 611 057	3407^3	49 189 183	7013^3
704 761	839^3	11 899 051	3449^3	52 265 671	7229^3

TABLE II (*Continued*)

Table of primes q of the form $q = (p^r - 1)/(p^d - 1)$, where p is a prime and r and d are positive integers.

q	p^r	q	p^r	q	p^r
52 613 263	7253^3	142 265 257	11927^3	256 240 057	16007^3
56 964 757	7547^3	142 408 423	11933^3	258 357 403	16073^3
62 149 573	7883^3	143 700 157	11987^3	262 209 281	127^5
62 433 703	7901^3	146 736 883	12113^3	263 396 671	16229^3
65 504 743	8093^3	147 464 593	12143^3	265 738 903	16301^3
67 757 593	8231^3	149 511 757	12227^3	269 665 663	16421^3
67 856 407	8237^3	150 099 253	12251^3	271 639 843	16481^3
70 350 157	8387^3	150 540 631	12269^3	274 018 363	16553^3
72 275 503	8501^3	155 588 203	12473^3	275 809 057	16607^3
72 991 393	8543^3	159 807 523	12641^3	277 605 583	16661^3
74 433 757	8627^3	159 959 257	12647^3	278 606 173	16691^3
75 160 231	8669^3	171 858 991	13109^3	285 660 703	16901^3
75 368 443	8681^3	173 277 733	13163^3	293 214 253	17123^3
76 413 823	8741^3	175 019 671	13229^3	300 450 223	17333^3
76 623 763	8753^3	177 728 893	13331^3	302 533 843	17393^3
77 572 057	8807^3	181 427 431	13469^3	305 175 781	5^{13}
80 344 333	8963^3	181 912 657	13487^3	305 463 007	17477^3
82 074 541	9059^3	182 236 501	13499^3	308 827 903	17573^3
86 927 653	9323^3	183 697 363	13553^3	309 672 007	17597^3
90 658 963	9521^3	185 327 383	13613^3	310 728 757	17627^3
90 887 623	9533^3	194 086 693	13931^3	318 176 407	17837^3
93 886 411	9689^3	198 457 657	14087^3	327 230 011	18089^3
94 468 681	9719^3	206 482 531	14369^3	329 404 351	18149^3
94 935 793	9743^3	210 815 881	14519^3	333 336 307	18257^3
95 052 751	9749^3	211 687 951	14549^3	333 774 631	18269^3
96 108 613	9803^3	221 042 557	14867^3	338 615 203	18401^3
103 052 953	10151^3	223 188 661	14939^3	350 869 093	18731^3
104 519 953	10223^3	223 547 353	14951^3	352 444 303	18773^3
105 873 811	10289^3	227 331 007	15077^3	357 191 101	18899^3
112 137 511	10589^3	228 236 557	15107^3	359 007 757	18947^3
113 028 793	10631^3	229 143 907	15137^3	361 513 183	19013^3
116 240 743	10781^3	229 507 351	15149^3	369 081 733	19211^3
124 802 413	11171^3	237 575 983	15413^3	373 243 081	19319^3
125 742 583	11213^3	241 103 257	15527^3	376 495 813	19403^3
126 416 293	11243^3	242 409 331	15569^3	386 574 583	19661^3
133 390 951	11549^3	244 656 523	15641^3	399 180 421	19979^3
135 059 263	11621^3	247 668 907	15737^3	399 660 073	19991^3
137 299 807	11717^3	249 561 007	15797^3	404 955 253	20123^3
138 709 507	11777^3	252 222 043	15881^3	408 828 181	20219^3
138 992 311	11789^3	253 557 853	15923^3	414 916 531	20369^3

As in the previous section $H(x)$ is the total number of primes of the form $(*)$ not exceeding x, and $G_3(x) = P_3((x - \frac{3}{4})^{1/2} - \frac{1}{2})$ is the number of primes of the form $p^2 + p + 1$ not exceeding x. (For the values of x listed in Table I, we actually have $G_3(x) = P_3(x^{1/2})$ except for the value $x = 10$.) The values in the last column of Table I are given to the nearest integer.

References

1. A. J. C. Cunningham and H. J. Woodall, *Factorisation of $y^n \mp 1$*, London, Hodgson, 1925.
2. L. E. Dickson, *On finite algebras*, Nachr. Ges. Wiss. Göttingen, 1905, pp. 358–393.
3. M. Kraitchik, *Recherches sur la théorie des nombres*, vol. 2, *Factorisation*, Paris, Gauthier-Villars, 1929.
4. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, vol. 1, Leipzig, Teubner, 1909, particularly §110.
5. ———, *Elementary number theory*, New York, Chelsea, 1958 (translation of the first half of the first volume of *Vorlesungen über Zahlentheorie*, Leipzig, Hirzel, 1927), particularly Theorems 116–120.
6. ———, *Vorlesungen über Zahlentheorie*, vol. 3, Leipzig, Hirzel, 1927, particularly pp. 125–142.
7. L. Poletti, *Le serie dei numeri primi appartenenti alle due forme quadratiche* (A) $n^2 + n + 1$ *e* (B) $n^2 + n - 1$ *per l'intervallo compreso entro* 121 *milioni, e cioè per tutti i valori di n fino a* 11000, Atti Accad. Naz. Lincei, Mem. Cl. Sci. Fis. Mat. Nat. (6), vol. 3 (1929), pp. 193–218.
8. K. Prachar, *Primzahlverteilung*, Berlin, Springer, 1957, particularly pp. 35–42.
9. C. L. Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math., vol. 66 (1944), pp. 122–136.
10. ———, *Sums of m^{th} powers of algebraic integers*, Ann. of Math. (2), vol. 46 (1945), pp. 313–339.
11. Rosemarie M. Stemmler, *The easier Waring problem in algebraic number fields*, Acta Arithmetica, vol. 6 (1961), pp. 447–468.
12. T. Tatuzawa, *On the Waring problem in an algebraic number field*, J. Math. Soc. Japan, vol. 10 (1958), pp. 322–341.
13. L. Tornheim, *Sums of n-th powers in fields of prime characteristic*, Duke Math. J., vol. 4 (1938), pp. 359–362.
14. J. P. Tull, *Dirichlet multiplication in lattice point problems*, Duke Math. J., vol. 26 (1959), pp. 73–80.
15. H. Weber, *Ueber Zahlengruppen in algebraischen Körpern*, Math. Ann., vol. 49 (1897), pp. 83–100.
16. ———, *Lehrbuch der Algebra*, 2nd ed., vol. 2, Braunschweig, Vieweg, 1899.

University of Illinois
Urbana, Illinois
Purdue Univeristy
Lafayette, Indiana