Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 43 (1988)
Heft: 5

Artikel: On the incongruence of consecutive fourth powers
Autor: Schumer, P. / Steinig, J.
DOI: https://doi.org/10.5169/seals-40810

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 28.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

On the incongruence of consecutive fourth powers

1. Introduction

In [1], Arnold, Benkoski and McCabe solve the following problem: Given an integer $n \geq 1$, what is the smallest positive integer k such that $1^2, 2^2, \ldots, n^2$ are all incongruent modulo k? Let $D(n)$ denote this integer; they show that

$$D(n) = \begin{cases} 1, & \text{if} \quad n = 1, \\ 2, & \text{if} \quad n = 2, \\ 9, & \text{if} \quad n = 4, \\ \min\{k \mid k \geq 2n \text{ and } k = p \text{ or } 2p \text{ with } p \text{ prime}\}, & \text{for all other } n. \end{cases}$$

Their proof, based on Bertrand's postulate, is neat and elementary. Their problem suggests the following generalization. Given integers $n \geq 1$ and $j \geq 1$, determine

$$D(j,n) := \min\{k \geq 1 \mid a^j \not\equiv b^j \pmod{k} \quad \text{if} \quad 1 \leq a < b \leq n\}.$$

If $j = 2$, $D(j,n) = D(n)$. In this article, we determine $D(2^h, n)$ for all $n \geq 1$ and $h \geq 2$. The proofs are elementary, and use an extension of Bertrand's postulate to primes $p \equiv 3 \pmod{4}$.
In the last section we mention what is known about $D(j,n)$ for other values of j.

2. The Theorem

We shall prove the following

Theorem. *For $h \geq 2$, we have*

$$D(2^h, n) = \begin{cases} 1, & \textit{if} \quad n = 1, \\ 2, & \textit{if} \quad n = 2, \\ 9, & \textit{if} \quad n = 4, \\ 18, & \textit{if} \quad n = 8, \\ \min\{k \mid k \geq 2n \textit{ and } k = p \textit{ or } 2p, \textit{ with } p \equiv 3 \pmod{4}\}, & \textit{for all other } n. \end{cases} \tag{2.1}$$

Here and in the sequel, p denotes a prime; we will always assume $h \geq 2$.
Following the notation in [1], we denote the quantity on the right side of (2.1) by $B(2^h, n)$. The proof that $D(2^h, n) = B(2^h, n)$ proceeds by establishing the following five lemmas.

Lemma 1. *$B(2^h, n) < 4n$ for $n \geq 1$.*

Lemma 2. *If $p > 2n$ and $p \equiv 3 \pmod{4}$, then $D(2^h, n) \leq p$.*

Lemma 3. *If* $2p \geq 2n$ *and* $p \equiv 3 \pmod 4$, *then* $D(2^h, n) \leq 2p$.

Lemma 4. $D(2^h, n) \geq 2n$ *for* $n \geq 3$.

Lemma 5. *If* $n \geq 5$, $n \neq 8$ *and* $2n \leq m < B(2^h, n)$, *then* $D(2^h, n) \neq m$.

3. The proofs

We shall use the following observation several times: if $h \geq 2$, $p \equiv 3 \pmod 4$ and

$$a^{2^h} \equiv b^{2^h} \pmod m, \tag{3.1}$$

with $m = p$, $2p$, p^2 or $2p^2$, then

$$a^{2^{h-1}} \equiv b^{2^{h-1}} \pmod m, \tag{3.2}$$

and by induction,

$$a^2 \equiv b^2 \pmod m. \tag{3.3}$$

Indeed, consider the case $m = p$:

$$a^{2^h} - b^{2^h} = (a^{2^{h-1}} - b^{2^{h-1}})(a^{2^{h-1}} + b^{2^{h-1}}),$$

the second factor on the right side is a sum of two squares and $p \equiv 3 \pmod 4$. Hence if p divides $(a^{2^{h-1}} + b^{2^{h-1}})$, then $p \mid a$ and $p \mid b$ [5, Theorem 367].
Similarly, if (3.1) holds (mod $2p$) then so does (3.2) because then $a \equiv b \pmod 2$.
And if (3.1) holds with $m = p^2$ or $m = 2p^2$, then (3.2) does also, since $p^2 \mid a^{2^{h-1}}$ if $p \mid a$ and $h \geq 2$.

Proof of Lemma 1. For $1 \leq n \leq 4$ and $n = 8$, $B(2^h, n) < 4n$ by inspection. For $n \geq 5$, $n \neq 8$, this inequality follows immediately from the existence, for each integer $x \geq 4$, of a prime $p \equiv 3 \pmod 4$ such that $x < p < 2x$. An elementary proof of this extension of Bertrand's postulate (and of similar results for other arithmetical progressions) was given by Erdös [4], after Breusch [3] had proved it using complex variable techniques.

Proof of Lemma 2. Suppose $D(2^h, n) > p$. Then, for some integers a and b with $1 \leq a < b \leq n$, (3.1) would hold with $m = p$. But then, since $p \equiv 3 \pmod 4$, we also would have (3.3) with $m = p$. And this is impossible, because $1 \leq b - a < a + b < 2n < p$.

Proof of Lemma 3. If $D(2^h, n) > 2p$ then (3.1) holds, with $m = 2p$, for some a, b with $1 \leq a < b \leq n$. But then $a^2 \equiv b^2 \pmod{2p}$, which is impossible since
$1 \leq b - a < a + b < 2n \leq 2p$.

Proof of Lemma 4. Clearly, $D(2^h, n) \geq 3$ if $n \geq 3$. Any integer k such that $3 \leq k < 2n$ can be written $k = a + b$, with $1 \leq a < b \leq n$. Then $a^{2^h} \equiv b^{2^h} \pmod{k}$, since $(a+b) \mid (a^{2^h} - b^{2^h})$; hence $D(2^h, n) \neq k$.

Proof of Lemma 5. By definition of $B(4, n)$, the assumption $2n \leq m < B(4, n)$ entails $m \neq p$ and $m \neq 2p$, if $p \equiv 3 \pmod 4$. We accordingly have 5 possibilities, if $n \geq 2$:

(1) $m = rs$, $r > s \geq 2$, $r \equiv s \pmod 2$,
(2) $m = 2rs$, $r > s \geq 3$, $r \equiv s \equiv 1 \pmod 2$,
(3) $m = p$ or $2p$, $p \equiv 1 \pmod 4$,
(4) $m = p^2$,
(5) $m = 2p^2$.

Since (3.2) implies (3.1) for any modulus m and any $h \geq 1$, it suffices to show that in each case there are integers a, b such that $1 \leq a < b \leq n$ and $a^2 \equiv b^2 \pmod m$ or $a^4 \equiv b^4 \pmod m$.
In cases (1) and (2), take $a = \frac{1}{2}(r - s)$, $b = \frac{1}{2}(r + s)$. Then $1 \leq a < b$ and $a^2 \equiv b^2 \pmod m$. Also, $\frac{1}{2}(r + s) \leq \frac{1}{4}rs + 1$ since $r \geq 2$ and $s \geq 2$ (write $2(r - s) \leq s(r - 2)$). Hence $b \leq \frac{1}{4}rs + 1 \leq \frac{1}{4}m + 1$; since $m < B(2^h, n) < 4n$, we have $b \leq n$.
In case (3), m is a sum of two squares [5, Theorem 366], say $m = a^2 + b^2$, with $1 \leq a < b$. Further, $b^2 < m < B(2^h, n) < 4n$, whence $b < n$ if $n \geq 4$. And $m = a^2 + b^2$ implies $a^4 \equiv b^4 \pmod m$.
In case (4), take $a = p$, $b = 2p$. Then $1 < a < b$ and $a^2 \equiv b^2 \pmod m$. Also, $b = 2p = 2\sqrt{m} < 4\sqrt{n}$, whence $b < n$ if $n \geq 16$.
In case (5), $a = p$ and $b = 3p$ satisfy $1 < a < b$ and $a^2 \equiv b^2 \pmod m$. And $b = 3\sqrt{m/2} < \sqrt{18n}$, whence $b < n$ if $n \geq 18$.
In order to complete the discussion of cases (4) and (5) we observe that $10 \leq m < 38$ if $5 \leq n \leq 17$, since $B(2^h, n)$ is non-decreasing (in n) and $B(2^h, 17) = 38$. If $10 \leq m < 38$ then $m = 25$ in case (4), $m = 18$ in case (5). But $D(2^h, n) \neq 25$ if $n \geq 4$ since $3^4 \equiv 4^4 \pmod{25}$, $D(2^h, n) \neq 18$ if $n \geq 9$ since $3^2 \equiv 9^2 \pmod{18}$, $D(2^h, n) \neq 18$ if $n \leq 7$ by Lemma 3.

Proof of the Theorem. By Lemmas 2 and 3 we have $D(2^h, n) \leq B(2^h, n)$ for $n \neq 1, 2, 4, 8$. By Lemmas 4 and 5, $D(2^h, n) \geq B(2^h, n)$ for $5 \leq n \leq 7$ and $n \geq 9$. This proves the theorem for $n \geq 5$, $n \neq 8$.
Trivially, $D(2^h, 1) = 1$ and $D(2^h, 2) = 2$; $D(2^h, 3) = 6$ by Lemmas 3 and 4. It remains to determine $D(2^h, 4)$ and $D(2^h, 8)$.
By Lemma 4, $D(2^h, 8) \geq 16$; $D(2^h, 8) \geq 18$ since $4^2 \equiv 8^2 \pmod{16}$ and $1^4 \equiv 4^4 \pmod{17}$. In fact, $D(2^h, 8) = 18$. Indeed, if (3.1) holds for $m = 18$, then (3.3) does also, hence $a^2 \equiv b^2 \pmod 9$ and $a \equiv b \pmod 2$. But if $a^2 \equiv b^2 \pmod 9$ and $1 \leq a < b \leq 8$ then $a + b = 9$, $a \not\equiv b \pmod 2$.
For $D(2^h, 4)$, Lemma 4 yields $D(2^h, 4) \geq 8$; and $D(2^h, 4) \neq 8$ since $2^4 \equiv 4^4 \pmod 8$. An argument similar to the one used for $D(2^h, 8)$ will show that $D(2^h, 4) = 9$ (start from (3.1) with $m = 9$).

4. Other results

The following table gives the values of $D(j,n)$ for $2 \leq j \leq 30$, $1 \leq n \leq 20$.

$j\backslash n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	1	2	6	9	10	13	14	17	19	22	22	26	26	29	31	34	34	37	38	41
3	1	2	3	5	5	6	10	10	10	10	11	15	15	15	15	17	17	22	22	22
4	1	2	6	9	11	14	14	18	19	22	22	31	31	31	31	38	38	38	38	43
5	1	2	3	5	5	6	7	10	10	10	13	13	13	14	15	17	17	19	19	21
6	1	2	6	10	10	17	17	17	22	22	22	29	29	29	34	34	34	41	41	41
7	1	2	3	5	5	6	7	10	10	10	11	13	13	14	15	17	17	19	19	21
8	1	2	6	9	11	14	14	18	19	22	22	31	31	31	31	38	38	38	38	43
9	1	2	3	5	5	6	10	10	10	10	11	15	15	15	15	17	17	22	22	22
10	1	2	6	9	10	13	14	17	19	23	23	26	26	29	34	34	34	37	38	43
11	1	2	3	5	5	6	7	10	10	10	11	13	13	14	15	17	17	19	19	21
12	1	2	6	11	11	22	22	22	22	22	22	46	46	46	46	46	46	46	46	46
13	1	2	3	5	5	6	7	10	10	10	11	13	13	14	15	17	17	19	19	21
14	1	2	6	9	10	13	14	17	19	22	22	26	26	31	31	34	34	37	38	41
15	1	2	3	5	5	6	10	10	10	10	15	15	15	15	15	17	17	23	23	23
16	1	2	6	9	11	14	14	18	19	22	22	31	31	31	31	38	38	38	38	43
17	1	2	3	5	5	6	7	10	10	10	11	13	13	14	15	17	17	19	19	21
18	1	2	6	10	10	17	17	17	22	22	22	29	29	29	34	34	34	41	41	41
19	1	2	3	5	5	6	7	10	10	10	11	13	13	14	15	17	17	19	19	21
20	1	2	6	9	14	14	14	18	19	23	23	38	38	38	38	38	38	38	38	43
21	1	2	3	5	5	6	10	10	10	10	11	15	15	15	15	17	17	22	22	22
22	1	2	6	9	10	13	14	17	19	22	22	26	26	29	31	34	34	37	38	41
23	1	2	3	5	5	6	7	10	10	10	11	13	13	14	15	17	17	19	19	21
24	1	2	6	11	11	22	22	22	22	22	22	46	46	46	46	46	46	46	46	46
25	1	2	3	5	5	6	7	10	10	10	13	13	13	14	15	17	17	19	19	21
26	1	2	6	9	10	13	14	17	19	22	22	26	26	29	31	34	34	37	38	41
27	1	2	3	5	5	6	10	10	10	10	11	15	15	15	15	17	17	22	22	22
28	1	2	6	9	11	14	14	18	19	22	22	31	31	31	31	38	38	38	38	46
29	1	2	3	5	5	6	7	10	10	10	11	13	13	14	15	17	17	19	19	21
30	1	2	6	10	10	17	17	17	23	23	23	29	29	29	34	34	34	46	46	46

Further computer assisted calculations have shown that $D(100,100) = 206$, $D(600,600) = 1223$, $D(1000,1000) = 2003$ and $D(2000,2000) = 4003$.
The following results are proved in [2] for sufficiently large n.
Let $p_1, \ldots, p_r$ be odd primes and $a_1, \ldots, a_r$ positive integers.

1. If $j = p_1^{a_1} \ldots p_r^{a_r}$, then

$$D(j,n) = \min\{k \mid k \geq n,\ k \text{ squarefree and not divisible by any } p \equiv 1 \pmod{p_i},\ i = 1, \ldots, r\}.$$

2. If $j = 2p_1^{a_1} \ldots p_r^{a_r}$, then

$$D(j,n) = \min\{k \mid k \geq 2n,\ k = p \text{ or } 2p \text{ with } p \not\equiv 1 \pmod{p_i},\ i = 1, \ldots, r\}.$$

3. If $j = 2^a p_1^{a_1} \dots p_r^{a_r}$ with $a \geq 2$, then

$$D(j,n) = \min \{k \mid k \geq 2n,\ k = p \text{ or } 2p \text{ with } p \not\equiv 1 \pmod{p_i},\ i = 1, \dots, r, \text{ and } p \equiv 3 \pmod 4\}.$$

In [6] a proof is given for $j = 3$ and $j = 6$, and all n, using the theory of binary quadratic forms.

P. Schumer, Department of
Mathematics and Computer Science,
Middlebury College

J. Steinig,
Section de Mathématiques
Université de Genève

REFERENCES

1 L. K. Arnold, S. J. Benkoski and B. J. McCabe: The Discriminator (A Simple Application of Bertrand's Postulate). Amer. Math. Monthly *92*, 275–277 (1985).
2 P. S. Bremser, P. D. Schumer and L. C. Washington: A Note on the Incongruence of Consecutive Integers to a Fixed Power, preprint.
3 R. Breusch: Zur Verallgemeinerung des Bertrandschen Postulates, dass zwischen x und $2x$ stets Primzahlen liegen. Math. Z. *34*, 505–526 (1932).
4 P. Erdös: Über die Primzahlen gewisser arithmetischer Reihen. Math. Z. *39*, 473–491 (1935).
5 G. H. Hardy and E. M. Wright: An Introduction to the Theory of Numbers. Oxford 1979.
6 P. Schumer: On the Incongruence of Consecutive Cubes, preprint.

© 1988 Birkhäuser Verlag, Basel 0013-6018/88/050145-05$1.50+0.20/0

Un problème de probabilité maximale

Dans un récent article [1], on trouve le théorème suivant:

Théorème: Si $X_1, \dots, X_n$ sont des variables aléatoires indépendantes, distribuées selon des lois géométriques de paramètres $r_1, \dots, r_n$, le maximum de la probabilité $P(X_1 + X_2 + \dots + X_n = i)$ est atteint, pour n et i donnés, lorsque $r_1 = \dots = r_n = i/(n+i)$.

Nous donnons ici une démonstration élémentaire du théorème. Soit F l'ensemble des lois de probabilités sur N avec la convolution $p * q(i) = \sum p(j) q(i-j)$. Soit $g_r(i) = s \cdot r^i$ (avec $s = 1 - r$) la loi géométrique de paramètre $r \geqq 0$ et $G_n = \{g_{r(1)} * g_{r(2)} * \dots * g_{r(n)}\}$ l'ensemble des convolutions de n lois géométriques.

Lemme 1: Si $p \in G_n$ et que l'on définit $\Delta p(i) = p(i) - p(i-1)$, il existe $i_0 = i_0(p)$ tel que $\Delta p(i) \geqq 0$ pour $i < i_0$ et $\Delta p(i) < 0$ pour $i \geqq i_0$ (unimodularité).