

MATHEMATICAL ASSOCIATION



supporting mathematics in education

3042. On Mersenne's Primes, Fermat's Primes and Even Perfect Numbers

Author(s): D. Suryanarayana

Source: *The Mathematical Gazette*, Vol. 46, No. 358 (Dec., 1962), pp. 319-320

Published by: The Mathematical Association

Stable URL: <http://www.jstor.org/stable/3611787>

Accessed: 24/03/2010 20:14

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=mathas>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.



The Mathematical Association is collaborating with JSTOR to digitize, preserve and extend access to *The Mathematical Gazette*.

<http://www.jstor.org>

3042. On Mersenne's primes, Fermat's primes and even perfect numbers

Theorem I. Let n be an odd integer > 1 . A necessary and sufficient condition for n to be a Mersenne's prime is that

$$p^2 - 1 \equiv 0 \pmod{\frac{1}{2}n(n+1)},$$

p being the product of all positive odd integers $< n$.

Theorem II. Let n be an even integer > 2 . A necessary and sufficient condition for $(n+1)$ to be a Fermat's prime is that

$$(p-1)(p^2+1) \equiv 0 \pmod{\frac{1}{2}n(n+1)},$$

p being the product of all positive odd integers $< n$.

Theorem III. For any integer $x > 3$ to be an even perfect number, it is necessary and sufficient that (i) x is a triangular number and (ii) $p^2 - 1 \equiv 0 \pmod{x}$, p being the product of all positive odd integers $< n$, where $x = \frac{1}{2}n(n+1)$ (the n th triangular number).

Proof of Theorem I. Suppose n is a Mersenne's prime, say $2^{r+1} - 1$.

$$p = 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2^{r+1} - 3) \equiv -(2^{r+1} - 2) \cdot -(2^{r+1} - 4) \cdot \dots \cdot -2 \pmod{2^{r+1} - 1}$$

$$\therefore p^2 \equiv -(2^{r+1} - 2)! \pmod{2^{r+1} - 1}$$

$$\equiv 1 \pmod{2^{r+1} - 1}, \text{ by Wilson's theorem.} \tag{1}$$

Now consider the two sets of numbers, viz; $1, 3, 5, \dots, 2^r - 1$ and $2^r + 1, 2^r + 3, \dots, 2^{r+1} - 3, 2^{r+1} - 1$. Each set is clearly a reduced residue system modulo 2^r . Therefore to each member l of the first set corresponds a unique member l' of the second set such that $ll' \equiv 1 \pmod{2^r}$. Taking the product of all such congruences (2^{r-1} congruences in number), we have

$$p(2^{r+1} - 1) \equiv 1 \pmod{2^r}$$

$$\therefore p^2 \equiv 1 \pmod{2^r} \tag{2}$$

Since $(2^r, 2^{r+1} - 1) = 1$, from (1) and (2) we see that

$$p^2 - 1 \equiv 0 \pmod{\frac{1}{2}n(n+1)}.$$

Thus the condition is necessary.

If $p^2 - 1 \equiv 0 \pmod{n(n+1)/2}$, it immediately follows that n is a prime and $n+1$ is a power of 2, since n is odd > 1 ; so that n is a Mersenne's prime. Hence the condition is sufficient.

Proof of Theorem II. Suppose $(n+1)$ is a Fermat's prime, say $2^{2^r} + 1$. Since n is an even integer > 2 , $r \geq 1$.

$$p = 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2^{2^r} - 1) \equiv -2^{2^r} \cdot -(2^{2^r} - 2) \cdot \dots \cdot -2 \pmod{2^{2^r} + 1}$$

$$\text{Since } r \geq 1, \quad p^2 \equiv (2^{2^r})! \pmod{2^{2^r} + 1}$$

$$\equiv -1 \pmod{2^{2^r} + 1} \text{ by Wilson's theorem.}$$

Using the same argument as in the proof of theorem I, we can prove that $p \equiv 1 \pmod{2^{2r-1}}$.

Thus we see that

$$(p - 1)(p^2 + 1) \equiv 0 \pmod{\frac{1}{2}n(n + 1)}$$

and so the condition is necessary.

If $(p - 1)(p^2 + 1) \equiv 0 \pmod{\frac{1}{2}n(n + 1)}$, it immediately follows that $(n + 1)$ is a prime and $\frac{1}{2}n$ is a power of 2, since n is even > 2 . By the well-known result that if $2^t + 1$ is a prime, then t is a power of 2, it follows that $(n + 1)$ is a Fermat's prime. Hence the condition is sufficient.

Proof of Theorem III. Suppose x is an even perfect number. It is well known that x must be of Euclid's type, namely $2^r(2^{r+1} - 1)$ where $2^{r+1} - 1$ is a prime. Clearly x is the $(2^{r+1} - 1)$ th triangular number, so that the condition (i) is satisfied and (ii) is also satisfied in virtue of Theorem I. Thus the conditions are necessary.

If $x > 3$ is a triangular number, say $\frac{1}{2}n(n + 1)$ and $p^2 - 1 \equiv 0 \pmod{x}$, p being the product of all positive odd integers $< n$, we shall prove that n is odd > 1 . Since $x > 3$, $n > 2$. Suppose if possible that n is even; then by the above congruence it is clear that $\frac{1}{2}n$ is a power of 2, say 2^r and $n + 1 = 2^{r+1} + 1$ is a prime. By the result already mentioned in the proof of theorem II, it follows that $(n + 1)$ is a Fermat's prime and hence $p^2 + 1 \equiv 0 \pmod{(n + 1)}$. But by hypothesis we have $p^2 - 1 \equiv 0 \pmod{(n + 1)}$. Therefore $(n + 1)$ must divide 2 which is a contradiction to the supposition that n is even. Thus n is odd > 1 . By theorem I, it follows that n is a Mersenne's prime; so that x is an even perfect number. Hence the conditions are sufficient.

*Department of Mathematics,
Andhra University,
Waltair, India*

D. SURYANARAYANA

3043. Volume of a triangular pyramid

Let O, P_1, P_2, P_3 be the vertices and V the volume. The following two determinantal formulae

$$36V^2 = OP_1^2 OP_2^2 OP_3^2 \begin{vmatrix} 1 & \cos(1, 2) & \cos(1, 3) \\ \cos(2, 1) & 1 & \cos(2, 3) \\ \cos(3, 1) & \cos(3, 2) & 1 \end{vmatrix} \quad (1)$$

and

$$36V^2 = \begin{vmatrix} OP_1^2 & (OP_1^2 + OP_2^2 - P_1P_2^2)/2 & (OP_1^2 + OP_3^2 - P_1P_3^2)/2 \\ (OP_2^2 + OP_1^2 - P_2P_1^2)/2 & OP_2^2 & (OP_2^2 + OP_3^2 - P_2P_3^2)/2 \\ (OP_3^2 + OP_1^2 - P_3P_1^2)/2 & (OP_3^2 + OP_2^2 - P_3P_2^2)/2 & OP_3^2 \end{vmatrix} \quad (2)$$