References

1. R. Courant, H. Robbins and I. Stewart, *What is Mathematics?: An elementary approach to ideas and methods*, Oxford University Press (1996) pp. 79-80.
2. K. Subramaniam, A new proof that the rationals are countable. *Math. Gaz.* **98** (July 2014) p. 345.
3. HomeSchoolmath.net. (n.d.). An easy proof that rational numbers are countable. Retrieved August 20, 2022, from https://www.homeschoolmath.net/teaching/rational-numbers-countable.php

10.1017/mag.2024.72 © The Authors, 2024
Published by Cambridge University Press on behalf of The Mathematical Association

RICHARD KAUFMAN
Office Expander
(www.OfficeExpander.com)
North Andover, MA, USA
e-mail: *rdkaufman01@gmail.com*

108.20 Euler's totient theorem and Fermat's little theorem are generalisations of one another!

Let us consider a non-familiar converse for the obvious fact that if $a \equiv 1 \pmod{n}$, then n divides $a^n - 1$, which is also related to Fermat's little theorem (briefly, Fermat's theorem). For example if $n = p$ is prime, then by Fermat's theorem, p divides $a^p - 1$ if, and only if, $a \equiv 1 \pmod{p}$. In fact, $a \equiv 1 \pmod{p}$ if, and only if, $a^p \equiv 1 \pmod{p^2}$. Indeed, for any natural numbers a, n, if $a \equiv 1 \pmod{n}$ then $a^n \equiv 1 \pmod{n^2}$ and by applying an induction on a natural number m we have $a^{n^m} \equiv 1 \pmod{n^{m+1}}$. In the last step of this induction, one may write

$$a^{n^{m+1}} - 1 = \left(a^{n^m} - 1\right)\left(a^{n^m(n-1)} + a^{n^m(n-2)} + \ldots + 1\right),$$

assuming $a^{n^m} \equiv 1 \pmod{n^{m+1}}$, by the induction hypothesis, and noticing that the sum in the previous parenthesis is divisible by n [note, still $a \equiv 1 \pmod{n}$], we then immediately infer that $a^{n^{m+1}} \equiv 1 \pmod{n^{m+2}}$. In this Note we like to formulate a few results related to the above non-familiar converse and obtain some useful consequences including the unusual fact in the title. Indeed, this fact is a rare occurrence between any two theorems in mathematics, even between the equivalent ones (see my concluding comments, briefly). Using the above simple facts, and invoking Fermat's theorem, one may observe that if we replace n by a prime number p in the above congruences, then $a^{p^m} \equiv 1 \pmod{p^{m+1}}$ if, and only if, $a \equiv 1 \pmod{p}$. In particular, if $p = 2$, then $a^{2^m} \equiv 1 \pmod{2^{m+2}}$ if, and only if, a is odd, where $m \geqslant 1$. We show that the latter two cases can be unified and obtained as consequences of either Corollary 1 or Corollary 2, below. Before presenting the results, let us recall that if p is the least prime divisor of a natural number n, then $(n, p - 1) = 1$. Motivated by this we define a *quasi-prime* number to be a natural number n such that $(n, p - 1) = 1$, where p is any prime divisor of n. It is evident that n is *quasi-prime* if, and

https://doi.org/10.1017/mag.2024.73 Published online by Cambridge University Press

only if, for, $p_1 < p_2 < \ldots < p_k$, the sequence of distinct prime divisors of n, $(p_i, p_j - 1) = 1$ for all $i \leqslant j$. For example, $n = p^m$, where p is prime and m a positive integer; $n = p^r q^s$, where r, s are natural numbers and $p < q$ are primes such that p does not divide $q - 1$ (note, in this case, the pair p, q can be any twin primes); or if the prime divisors of n are all of the form of Fermat primes, i.e. of the form $2^{2^k} + 1$, where k is a nonnegative integer. It is clear that n is an even *quasi-prime* number if, and only if, $n = 2^m$ for some natural number m. Using the above observations, we are now ready to present our results.

Theorem A: Let n be a natural number and a be a positive integer. Then $a^n \equiv 1 \pmod{q_n n}$, where n is even, $q_n = 2q$ (resp., n is odd, $q_n = q$), and q is the product of distinct prime divisors of n if, and only if, for any prime divisor p of n, $a^{d_p} \equiv 1 \pmod{p}$, with $d_p = (n, p - 1)$.

Proof: Let $a^n \equiv 1 \pmod{q_n n}$. Clearly, $a^n \equiv 1 \pmod{p}$ for any prime divisor p of n and $(a, p) = 1$, hence by Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$. Consequently, $a^{d_p} \equiv 1 \pmod{p}$, where $d_p = (n, p - 1)$. Conversely, let $n = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$ be the prime factorisation of n. Then by our assumption and by what we have already observed earlier, for any p_i we must have $a^{d_{p_i}} \equiv 1 \pmod{p_i}$ with $d_{p_i} = (n, p_i - 1)$ and hence $a^{d_{p_i} p_i^{m_i}} \equiv 1 \pmod{p_i^{m_i+1}}$ for any i. Now if p_j is even (i.e. $p_j = 2$) then $a^{d_{p_j} p_j^{m_j}} \equiv 1 \pmod{p_j^{m_j+2}}$. But, $(d_{p_i}, p_i^{m_i}) = 1$ for any i, and hence n is divisible by $d_{p_i} p_i^{m_i}$. Consequently, $a^n \equiv 1 \pmod{p_i^{m_i+1}}$ for any i and if p_j is even, then $a^n \equiv 1 \pmod{p_j^{m_j+2}}$. This implies that if n is odd, $a^n \equiv 1 \pmod{p_1^{m_1+1} p_2^{m_2+1} \ldots p_k^{m_k+1}}$, i.e. $a^n \equiv 1 \pmod{q_n n}$, where $q_n = q$ and in the case n is even, we may take $p_1 = 2$ and hence we have $a^n \equiv 1 \pmod{p_1^{m_1+2} p_2^{m_2+1} \ldots p_k^{m_k+1}}$, i.e. $a^n \equiv 1 \pmod{q_n n}$, where $q_n = 2q$, and we are done.

The next corollaries are now immediate.

Corollary 1: Let n be any *quasi-prime* number and a be a positive integer. Then $a^n \equiv 1 \pmod{q_n n}$, where n is even, $q_n = 2q$ (and similarly, where n is odd, $q_n = q$) and q is the product of distinct prime divisors of n if, and only if, for any prime divisor p of n, $a \equiv 1 \pmod{p}$.

Corollary 2: Let n be a *quasi-prime* number which is square-free and a, m be natural numbers. Then $a^{n^m} \equiv 1 \pmod{n^{m+1}}$, where n is odd (resp., $a^{n^m} \equiv 1 \pmod{n^{m+2}}$, where n is even (i.e., $n = 2$)) if, and only if, $a \equiv 1 \pmod{n}$.

The following theorem, together with its remark, clearly show that Fermat's theorem is equivalent to a generalisation of Euler's theorem. Although, its proof is similar to the proof of Theorem A, it is given for the sake of completeness.

https://doi.org/10.1017/mag.2024.73 Published online by Cambridge University Press

Theorem B: Let m, n be positive integers such that whenever p^k divides n, $p^{k-1}(p-1)$ divides m, where p is a prime number and k is a positive integer (e.g. $m = \phi(n)$, where ϕ is Euler's function). Then $a^m \equiv 1 \pmod{n}$ if, and only if, for any prime divisor p of n, $a^{d_p} \equiv 1 \pmod{p}$, with $d_p = (m, p-1) = p-1$.

Proof: Let $a^m \equiv 1 \pmod{n}$ and p be a prime divisor of n, then $(a, p) = 1$. Now by Fermat's theorem and the assumption that $p-1$ divides m, we immediately infer that $a^{d_p} \equiv 1 \pmod{p}$, where $d_p = (m, p-1) = p-1$.

Conversely, let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ be the prime factorisation of n. By our assumption $a^{d_{p_i}} \equiv 1 \pmod{p_i}$ for each i, where $1 \leqslant i \leqslant k$. Now by the observations that we started off with, we have $a^{d_{p_i} p_i^{\alpha_i - 1}} \equiv 1 \pmod{p_i^{\alpha_i}}$ for each i. Since $(d_{p_i}, p_i^{\alpha_i - 1}) = 1$ we infer that $d_{p_i} p_i^{\alpha_i - 1}$ divides m, hence $a^m \equiv 1 \pmod{p_i^{\alpha_i}}$ for each i. Consequently, we have $a^m \equiv 1 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}$ and we are done.

Remark: There are infinitely many positive pairs of integers, m, n, with the above property, in the statement of Theorem B, satisfying $m < \phi(n)$. To this end, let $n = 2^r \times 3^s \times 7^t \times 13^u$ and $m = 2^{r-1} \times 3^{s-1} \times 7^{t-1} \times 13^{u-1}$, where the integers s, t, u are greater than 1 and $r > 2$. One may choose other primes similar to 2, 3 , 7 and 13 with putting appropriate restrictions on r, s, t, u. For example, we may replace 13 by 17 and assuming that $r > 4$ or even one may change the number of above primes. Or, simply let $F_i = 2^{k_i} + 1$, where $i = 1, 2, \dots, s$, be Fermat prime numbers with $F_i < F_j$ for $i < j$, then we may put $n = 2^t \left(\prod_{i=1}^{s} F_i^{d_i}\right)$, $m = 2^{t-1} \left(\prod_{i=1}^{s} F_i^{d_i - 1}\right)$, where t, d_i are positive integers with $t > k_s$ and $d_i > 1$ for all i. Clearly, $m < \phi(n)$ and m, n have the above property in the statement of Theorem B.

The comments and observations preceding Theorem A, have also some manifest consequences as follows. Let m, n be two natural numbers with the same primes in their prime factorisations (or just assuming, m, n share the same minimal prime divisor), then $m \nmid 2^n - 1$ (for otherwise, let $m \mid 2^n - 1$, then by taking p to be the least prime divisor of m we must have $(2, p) = 1$, $(n, p-1) = (m, p-1) = 1$, but $p \mid 2^n - 1$ with $p \mid 2^{p-1} - 1$ imply that $p \mid 2^{(n,p-1)} - 1$, which is absurd, for $(n, p-1) = 1$). In particular, $n \nmid 2^n - 1$. More generally $m \nmid a^n - 1$, where a is a natural number with $a \not\equiv 1 \pmod{p}$ for the least prime divisor p of n. Moreover, if n is also a *quasi-prime* number, then for any natural number q, $q \nmid a^n - 1$, where $a \neq 1$ is a natural number with $a \leqslant p$ for some prime divisor p of (n, q). Although, as we have already emphasised above that Theorem B, manifestly shows that Fermat's theorem is a generalisation of Euler's theorem, however we like to make the next comments, too. A conspicuous consequence of Theorem B, is the non-emphasised fact in the literature, to wit, "Euler's theorem generalises Fermat's theorem and vice versa". In almost all the elementary textbooks on number theory, the authors usually claim that Euler's theorem is a generalisation of Fermat's theorem. Whereas in Theorem B, it is explicitly shown that the two theorems are, in fact, equivalent. Indeed, Fermat's theorem plays a key role in both the statement

https://doi.org/10.1017/mag.2024.73 Published online by Cambridge University Press

and the proof of the theorem. However, we should remind the reader that when two theorems, P, Q say, are equivalent (i.e, a proof of P can be deduced from Q and vice versa) they need not be generalisations of one another. For example, Pythagorean theorem and Law of Cosines are equivalent, and the latter is a generalisation of the former but not necessarily vice versa (note, no generalisation of Law of Cosines is known in the literature that is proved via Pythagorean theorem, up to now). We like to remind the reader that in [2, Prob. 15(c). p. 58] it is observed that Euler's theorem can be deduced from Fermat's theorem. However, in [2], and also in the literature, in general, the peculiar and simple fact that Fermat's theorem is, indeed, a generalisation of Euler's theorem too, is overlooked (note, as John Conway once said, see [1], [3]: All the easy things, at first sight, appear to have been said already, but you can find that they have not been said). Finally, we would like to record the following equivalence, also as a corollary to Theorem B.

Corollary 3: The following theorems are equivalent.

(1) Fermat's theorem.

(2) Euler's theorem.

Acknowledgment

The author would like to thank the referee and the Editor for reading this Note carefully and giving useful comments.

References

1. O.A.S. Karamzadeh, A very elementary short proof of Conway's little theorem, *Math. Gaz.*, **102** (November 2018) pp. 496-497.
2. I.M. Vinogradov, *Elements of number theory*, Translated from the Fifth Revised Edition by Saul Kravetz, Dover Publication (1954).
3. O.A.S. Karamzadeh, An elementary-minded mathematician, special issue of the *Mathematical Intelligencer*, 31 May (2021) pp. 76-78.

10.1017/mag.2024.73 © The Authors, 2024
Published by Cambridge University Press on behalf of The Mathematical Association

O.A.S. KARAMZADEH
Department of Mathematics, Shahid Chamran University, Ahvaz, Iran
e-mail: *karamzadeh@ipm.ir*

108.21 An amazing quartet of integrals

Introduction: Some time ago I stumbled upon the following four related integral representations of well-known mathematical constants:

$$\pi^2 = 2J(-2),\ \zeta(3) = \tfrac{2}{7}J(-1),\ \pi^3 = 8J(0),\ G = \tfrac{1}{4}J(1)$$

where

$$J(k) = \int_0^{\frac{\pi}{2}} \operatorname{arctanh}^2(\cos t)\cos^k t\ dt$$