INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 4 (2004), #A22

THE SQUARE OF THE FERMAT QUOTIENT

Andrew Granville
Département de Mathématiques et statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal QC H3C 3J7, Canada
andrew@dms.umontreal.ca

Received: 4/13/04, Revised: 10/20/04, Accepted: 11/15/04, Published: 11/30/04

1. Introduction

Fermat quotients, numbers of the form $(a^{p-1}-1)/p$, played an important rôle in the study of cyclotomic fields and Fermat's Last Theorem [2]. They seem to appear in many surprising identities, one of the most delightful of which is Glaisher's observation that

$$\frac{2^{p-1}-1}{p} \equiv -\frac{1}{2}\left(\frac{2^1}{1}+\frac{2^2}{2}+\dots+\frac{2^{p-1}}{(p-1)}\right) \pmod{p}. \tag{1}$$

Recently Skula conjectured that

$$\left(\frac{2^{p-1}-1}{p}\right)^2 \equiv -\left(\frac{2^1}{1^2}+\frac{2^2}{2^2}+\dots+\frac{2^{p-1}}{(p-1)^2}\right) \pmod{p}. \tag{2}$$

It is stunning that such a simple but elegant generalization of (1) should have remained unnoticed for so long. In this note we prove (2), and indeed a further generalization.

One might hazard a guess that the ratio

$$\left(\frac{2^{p-1}-1}{p}\right)^k \Big/ \left(\frac{2^1}{1^k}+\frac{2^2}{2^k}+\dots+\frac{2^{p-1}}{(p-1)^k}\right) \pmod{p} \tag{3}$$

should also be a simple fixed rational number for other values of k, but calculations reveal that this is probably not the case.

We will present two proofs of (2), one a substantial simplification of our original proof due to the anonymous referee, the other a different simplification, but both of which contain formulas that are perhaps of independent interest.

2. The main results

Let p be a fixed prime > 3. Define

$$q(x) = \frac{x^p - (x-1)^p - 1}{p}, \text{ with } g(x) = \sum_{i=1}^{p-1} \frac{x^i}{i} \text{ and } G(x) = \sum_{i=1}^{p-1} \frac{x^i}{i^2}.$$

(Here, and throughout, x is a variable, and the results below are proved for polynomials in x; of course one may substitute in integers for x to obtain integer congruences.) Standard arguments give that $G(1) \equiv 0 \pmod p$. Since $1/r + 1/(p-r) = p/r(p-r)$ thus $2g(1) \equiv -pG(1) \equiv 0 \pmod{p^2}$. Also $G(-1) = \sum_{1 \le j \le (p-1)/2} (1/(2j)^2 - 1/(p-2j)^2) \equiv 0 \pmod p$.

We will prove the functional equation

$$G(x) \equiv G(1-x) + x^p G(1-1/x) \pmod{p}, \tag{4}$$

as well as the two "mod p–identities"

$$q(x)^2 \equiv -2x^p G(x) - 2(1-x^p)G(1-x) \pmod p \tag{5}$$

and

$$-G(x) \equiv \frac{1}{p}(q(x) + g(1-x)) \pmod p \tag{6}$$

which lead to two different proofs of (2): Substituting $x = 2$ into (5) and then into (6) we obtain

$$q(2)^2 \equiv -2^{p+1}G(2) - 2(1-2^p)G(-1) \equiv -4G(2) \pmod p$$

which is (2), and then

$$-G(2) \equiv \frac{1}{p}(q(2) + g(-1)) \pmod p$$

which gives (2) from Glaisher's result [1] that $g(-1) \equiv -q(2) + pq(2)^2/4 \pmod{p^2}$.

3. Proofs

We begin with the trivial observation that $\binom{p-1}{j}(-1)^j \equiv 1 \pmod p$ for all $0 \le j \le p-1$. Then

$$q'(x) = x^{p-1} - (x-1)^{p-1} = -\sum_{j=0}^{p-2} \binom{p-1}{j} (-x)^j \equiv -\sum_{i=1}^{p-1} x^{i-1} = -g'(x) \pmod p.$$

This, together with the fact that $q(x)$ and $g(x)$ both have degree $< p$, implies that $q(x)+g(x) \equiv c_0 \pmod p$ for some constant c_0. Substituting in $x = 0$ we discover that $c_0 \equiv 0 \pmod p$ and so

$$q(x) + g(x) \equiv 0 \pmod p. \tag{7}$$

It is immediate from their definitions that $q(x) = q(1-x)$ and $g(x) \equiv -x^p g(1/x) \pmod p$. From these observations and (7) we deduce that $g(x) \equiv -q(x) = -q(1-x) \equiv g(1-x) \pmod p$ and $x^p g(1-1/x) \equiv x^p g(1/x) \equiv -g(x) \pmod p$. Now $G'(x) = g(x)/x$ and so

$$\begin{aligned}\frac{d}{dx}(G(1-x) + x^p G(1-1/x)) &\equiv -\frac{g(1-x)}{(1-x)} + x^p \frac{g(1-1/x)}{x^2(1-1/x)} \\ &= \frac{xg(1-x) + x^p g(1-1/x)}{x(x-1)} \equiv \frac{g(x)}{x} = G'(x) \pmod p,\end{aligned}$$

and therefore $G(x) - G(1-x) - x^p G(1-1/x) \equiv c_1 \pmod p$ for some constant c_1. Substituting in $x = 1$ we discover that $c_1 \equiv 0 \pmod p$ and so (4) holds.

Similarly, from the above, we have

$$\begin{aligned}\frac{d}{dx} q(x)^2 = 2q(x)q'(x) &\equiv -2g(x)\left(x^{p-1} - \sum_{j=0}^{p-1} x^j\right) \equiv -2x^p \frac{g(x)}{x} + 2(1-x^p)\frac{g(1-x)}{(1-x)} \\ &\equiv -2x^p G'(x) - 2(1-x^p)G'(1-x) \\ &\equiv \frac{d}{dx}(-2x^p G(x) - 2(1-x^p)G(1-x)) \pmod p.\end{aligned}$$

Therefore $q(x)^2 + 2x^p G(x) + 2(1-x^p)G(1-x) \equiv c_2 + c_3 x^p \pmod p$ since this polynomial has degree $< 2p$. Substituting in $x = 0$ and $x = 1$ we discover that $c_2 \equiv c_3 \equiv 0 \pmod p$ and we have proved (5).

Finally note that

$$\begin{aligned}\sum_{r=1}^{p-1} \frac{(1-x)^r - 1}{r} &= \sum_{j=1}^{p-1}\left(\sum_{r=1}^{p-1}\binom{r-1}{j-1}\right)\frac{(-x)^j}{j} = \sum_{j=1}^{p-1}\binom{p-1}{j}\frac{(-x)^j}{j} \\ &= \sum_{j=1}^{p-1}\left(\binom{p}{j} - \binom{p-1}{j-1}\right)\frac{(-x)^j}{j} \\ &= p\sum_{j=1}^{p-1}\left\{(-1)^j\binom{p-1}{j-1}\right\}\frac{x^j}{j^2} + \frac{(x-1)^p - x^p + 1}{p},\end{aligned}$$

which implies (6), since each $(-1)^{j-1}\binom{p-1}{j-1} \equiv 1 \pmod p$ and as $g(1) \equiv 0 \pmod p$.

Acknowledgements Thanks to Ladja Skula for finding this beautiful congruence, Takashi Agoh for informing me of Skula's conjecture and the anonymous referee for helping simplify my original proof.

References

1. J.W.L. Glaisher, *On the residues of the sums of products of the first* $p-1$ *numbers and their powers to modulus* p^2 *or* p^3, Quart. J. Math. Oxford **31** (1900), 321–353.

2. Paulo Ribenboim, *Thirteen lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.