

A congruence for the coefficients in a series for π

by

SCOTT AHLGREN (Urbana, IL)

1. Introduction. In [N-S], M. Newman and D. Shanks study properties of a sequence $\{a(n)\}$ which arises in earlier work of Shanks [S] on rapidly converging series for π . In an appendix to the paper, D. Zagier uses the theory of modular forms to obtain asymptotic information about the $a(n)$ and to prove a congruence for the $a(n)$ modulo 3. Zagier also records a conjectural congruence for the $a(n)$ modulo 5; the purpose of this note is to prove the conjectured congruence.

Throughout, we will assume that z is a variable of the upper half-plane, that $q := e^{2\pi iz}$, and that

$$U(z) := q \prod_{n=1}^{\infty} (1 + q^n)^{24}.$$

The integers $a(n)$ considered in [N-S] are defined via the relation

$$(1) \quad \log \left\{ \prod_{n=1}^{\infty} (1 + q^n) \right\} = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{a(n)}{n} U^n$$

(see equations (12) and (13) of [N-S]).

Differentiating (1), we find that

$$\frac{U'(z)}{U(z)} \sum_{n=1}^{\infty} (-1)^{n-1} a(n) U(z)^n = \frac{1}{24} \frac{d}{dz} \log \left(\frac{U(z)}{q} \right) = \frac{1}{24} \left(\frac{U'(z)}{U(z)} - 2\pi i \right).$$

Therefore, if $f(z)$ is the modular form of weight two on $\Gamma_0(2)$ defined by

$$f(z) := \frac{1}{2\pi i} \frac{U'(z)}{U(z)} = 1 + 24 \sum_{n=1}^{\infty} \sum_{\substack{d|n \\ d \text{ odd}}} dq^n,$$

2000 *Mathematics Subject Classification*: 11B50, 11F33.
The author is supported by NSF grant DMS-0134577.

we see that the integers $a(n)$ can be defined via the relation

$$(2) \quad \frac{1}{f(z)} = 1 + 24 \sum_{n=1}^{\infty} (-1)^n a(n) U(z)^n$$

(cf. equation (2) of Zagier's appendix to [N-S]). This definition will be more suitable for our purpose.

Zagier recorded the following conjectural congruence modulo 5:

$$(3) \quad a(n) \equiv \begin{cases} a(n/5) & \text{if } 5 \mid n, \\ 0 & \text{if } n = 10r + \delta, \delta = 6, 7, 8, 9, \\ \delta \binom{2r}{r}^3 & \text{if } n = 10r + \delta, \delta = 1, 2, 3, 4. \end{cases}$$

We remark that the congruence $a(5n) \equiv a(n) \pmod{5}$ is a special case of a general identity proved in [N-S] (see (20) in that work). For brevity, we will not reprove it here. In the next section we will prove the remaining two assertions in (3).

2. Proof of the congruence. If $E_4(z)$ denotes the usual weight four Eisenstein series

$$E_4(z) := 1 + 240 \sum_{n=1}^{\infty} \sum_{d \mid n} d^3 q^n,$$

then, using the interpretation of U and f as modular forms on the congruence subgroup $\Gamma_0(2)$, Zagier [N-S] showed that

$$\frac{E_4(z)}{f(z)^2} = \frac{1 + 256U(z)}{1 + 64U(z)}.$$

If we write $f(z) = \tilde{f}(U)$ and $E_4(z) = \tilde{E}_4(U)$, then, since $\tilde{E}_4(U) \equiv 1 \pmod{5}$, we see that

$$(4) \quad \frac{1}{\tilde{f}(U)^2} \equiv \frac{1 + U}{1 - U} \pmod{5}$$

(here and throughout, we view our series as elements of the ring of power series in U whose coefficients are rational and 5-integral; by a congruence between such series we mean a term-by-term congruence between the coefficients).

Define the 5-integral rational numbers $c(n)$ by

$$(5) \quad 1 + \sum_{n=1}^{\infty} c(n) U^n = \left(\frac{1 + U}{1 - U} \right)^{1/2}.$$

Then (4) and the definition (2) show that for all $n \geq 1$ we have

$$(6) \quad c(n) \equiv (-1)^{n+1} a(n) \pmod{5}.$$

We shall require Lucas's Theorem, which states that if n and m are non-negative integers whose least non-negative residues modulo 5 are n_0, m_0 , respectively, then

$$(7) \quad \binom{n}{m} \equiv \binom{n_0}{m_0} \binom{\lfloor n/5 \rfloor}{\lfloor m/5 \rfloor} \pmod{5}.$$

Using (7) and induction, we can verify that for all $r \geq 0$ we have

$$(8) \quad \binom{2r}{r}^3 \equiv (-1)^r \binom{2r}{r} \pmod{5}.$$

In fact, we see that something slightly stronger is true. Namely, if ν_d ($0 \leq d \leq 4$) denotes the number of occurrences of the digit d in the expansion of r in base 5, then $\binom{2r}{r}$ is congruent modulo 5 to 2^{ν_1} in the case when $\nu_3 = \nu_4 = 0$, and is otherwise congruent to 0.

Combining (3), (6) and (8), we see that to prove the conjecture, it will suffice to prove the following statements:

$$(9) \quad c(n) \equiv 0 \pmod{5} \quad \text{if } n = 10r + \delta, \delta = 6, 7, 8, 9,$$

$$(10) \quad c(n) \equiv (-1)^{n+r+1} \delta \binom{2r}{r} \pmod{5} \quad \text{if } n = 10r + \delta, \delta = 1, 2, 3, 4.$$

Using (5), we find that

$$(11) \quad \begin{aligned} 1 + \sum_{n=1}^{\infty} c(n)U^n &= (1 + U)(1 - U^2)^{-1/2} \\ &= (1 + U) \sum_{k=0}^{\infty} \binom{-1/2}{k} (-1)^k U^{2k}. \end{aligned}$$

It follows from (11) that

$$(12) \quad c(n) = c(n - 1) \quad \text{if } n \text{ is odd,}$$

$$(13) \quad c(n) = \frac{1}{2^{n-1}} \binom{n-1}{n/2} \quad \text{if } n \geq 2 \text{ is even.}$$

Using (12), we see that to prove (9) we need only consider the cases $\delta = 6, 8$. If $n = 10r + 6$, for example, then (13) and (7) show that

$$c(n) = \frac{1}{2^{10r+5}} \binom{10r+5}{5r+3} \equiv 0 \pmod{5}.$$

We can prove that $c(10r + 8) \equiv 0 \pmod{5}$ with a similar argument, and may therefore conclude that (9) is true.

We proceed to (10). Suppose first that $n = 10r + 1$. Then, using (7) and (12), we have

$$\begin{aligned} c(n) = c(10r) &= \frac{1}{2^{10r-1}} \binom{10r-1}{5r} \\ &\equiv (-1)^r \cdot 2 \binom{4}{0} \binom{2r-1}{r} \equiv (-1)^{n+r+1} \binom{2r}{r} \pmod{5}, \end{aligned}$$

as desired.

Similar arguments apply in the cases when $\delta = 2, 3, 4$ (the first two can be combined using (12)), and we omit the details here for brevity. We conclude that (10), and therefore the original conjecture (3), are true.

Acknowledgments. The author thanks the referee for suggesting several ways to improve the exposition in this paper.

References

- [N-S] M. Newman and D. Shanks (with an appendix by D. Zagier), *On a sequence arising in series for π* , Math. Comp. 42 (1984), 199–217.
- [S] D. Shanks, *Dihedral quartic approximations and series for π* , J. Number Theory 14 (1982), 397–423.

Department of Mathematics
University of Illinois
Urbana, IL 61801, U.S.A.
E-mail: ahlgren@math.uiuc.edu

*Received on 23.10.2001
and in revised form on 7.8.2002*

(4134)