SQUARE APPLICATIONS, I

KEITH CONRAD

1. Introduction

Numerical data suggest the following conjectures:

$$\begin{aligned}
-1 \equiv \Box \bmod p &\iff p = 2 \text{ or } p \equiv 1 \bmod 4,\\
2 \equiv \Box \bmod p &\iff p = 2 \text{ or } p \equiv 1, 7 \bmod 8,\\
-2 \equiv \Box \bmod p &\iff p = 2 \text{ or } p \equiv 1, 3 \bmod 8,\\
3 \equiv \Box \bmod p &\iff p = 2, 3 \text{ or } p \equiv 1, 11 \bmod 12,\\
-3 \equiv \Box \bmod p &\iff p = 2, 3 \text{ or } p \equiv 1 \bmod 3,\\
5 \equiv \Box \bmod p &\iff p = 2, 5 \text{ or } p \equiv 1, 4 \bmod 5.
\end{aligned}$$

As an illustration of what such equivalences are good for, we use them to extend Euclid's proof of the infinitude of the primes to proofs of the infinitude of primes in certain arithmetic progressions.

2. Extending Euclid's proof of the infinitude of the primes

Recall that an arithmetic progression is a sequence of numbers with a common difference between successive terms. It has the form $\{a, a+m, a+2m, a+3m, a+4m, \dots\}$. For example, the (positive) odd numbers are an arithmetic progression with $a = 1$ and $m = 2$. We will focus on arithmetic progressions where $a > 0$ and $m > 0$. In the language of congruences, an arithmetic progression is the set of (positive) integers satisfying a congruence condition $n \equiv a \bmod m$. Following the strategy of Euclid's proof that there are infinitely many primes, we will use square patterns to show for some special choices of a and m that there are infinitely many primes $p \equiv a \bmod m$.

Actually, our first two adaptations of Euclid's proof won't use any square patterns.

Theorem 2.1. *There are infinitely many primes $p \equiv 2 \bmod 3$.*

Proof. One such prime is 2. If $p_1, \dots, p_r$ are primes $\equiv 2 \bmod 3$, let

$$N = 3p_1p_2\cdots p_r - 1 > 1.$$

Then N is not divisible by 3 or by any of $p_1, \dots, p_r$. Since $N \equiv -1 \equiv 2 \bmod 3$, the prime divisors of N are not all $\equiv 1 \bmod 3$ (otherwise $N \equiv 1 \bmod 3$). Therefore N has a prime divisor p which is $\equiv 2 \bmod 3$. This prime is different from $p_1, \dots, p_r$, so there are infinitely many primes $\equiv 2 \bmod 3$. □

Theorem 2.2. *There are infinitely many primes $p \equiv 3 \bmod 4$.*

Proof. One such prime is 3. If $p_1, \dots, p_r$ are primes $\equiv 3 \bmod 4$, let

$$N = 4p_1p_2\cdots p_r - 1 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \ldots, p_r$. Since $N \equiv -1 \equiv 3 \bmod 4$, the prime divisors of N are not all $1 \bmod 4$ (otherwise $N \equiv 1 \bmod 4$). Therefore N has a prime divisor p which is $\equiv 3 \bmod 4$. This prime is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 3 \bmod 4$. □

The proofs of Theorems 2.1 and 2.2 relied on there being only two units modulo 3 and modulo 4. For $m > 2$ with $m \neq 3, 4$ or 6, there are more than two units modulo m (that is, there are units other than $\pm 1 \bmod m$). To extend Euclid's proof to new cases of $a \bmod m$, we will use quadratic expressions to define N in the proof (by comparison, the formula for N in Theorems 2.1 and 2.2 are linear in the product $p_1 \cdots p_r$). The conjectures at the start about squares modulo p will get used, giving motivation for proving those conjectures.

Theorem 2.3. *There are infinitely many primes* $p \equiv 1 \bmod 4$.

Proof. One such prime is 5. If $p_1, \ldots, p_r$ are primes $\equiv 1 \bmod 4$, let

$$N = (2p_1p_2 \cdots p_r)^2 + 1 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \ldots, p_r$. Let p be a prime factor of N, so $-1 \equiv \square \bmod p$. Therefore, since $p \neq 2$, our knowledge of when $-1 \equiv \square \bmod p$ tells us $p \equiv 1 \bmod 4$. This prime is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 1 \bmod 4$. □

Theorem 2.4. *There are infinitely many primes* $p \equiv 1 \bmod 3$.

Proof. One such prime is 7. If $p_1, \ldots, p_r$ are primes $\equiv 1 \bmod 3$, let

$$N = (2p_1p_2 \cdots p_r)^2 + 3 > 1.$$

Then N is not divisible by 2, 3, or any of $p_1, \ldots, p_r$. Let p be a prime factor of N, so $-3 \equiv \square \bmod p$. Therefore, since $p \neq 2$ or 3, the conjecture about when $-3 \equiv \square \bmod p$ tells us $p \equiv 1 \bmod 3$. This prime is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 1 \bmod 3$. □

Theorem 2.5. *There are infinitely many primes* $p \equiv 4 \bmod 5$.

Proof. One such prime is 19. If $p_1, \ldots, p_r$ are primes $\equiv 4 \bmod 5$, let

$$N = (2p_1p_2 \cdots p_r)^2 - 5 > 1.$$

Then N is not divisible by 2, 5, or any of $p_1, \ldots, p_r$. Let p be any prime factor of N, so $5 \equiv \square \bmod p$. Therefore, since $p \neq 2$ or 5, the conjecture about when $5 \equiv \square \bmod p$ tells us $p \equiv 1$ or $4 \bmod 5$: all prime factors of N are $1 \bmod 5$ or $4 \bmod 5$. To show N has a prime factor which is $4 \bmod 5$ we argue by contradiction. If every prime factor of N is $1 \bmod 5$, then $N \equiv 1 \bmod 5$, but in fact $N \equiv 4 \bmod 5$ since $p_i^2 \equiv 1 \bmod 5$ for all i. (Here we use $p_i \equiv 4 \bmod 5$.) Therefore some prime factor of N is not $1 \bmod 5$. The only option left is that this prime factor is $4 \bmod 5$. This prime is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 4 \bmod 5$. □

Theorem 2.6. *There are infinitely many primes* $p \equiv 3 \bmod 8$.

Proof. One such prime is 3. If $p_1, \ldots, p_r$ are primes $\equiv 3 \bmod 8$, let

$$N = (p_1p_2 \cdots p_r)^2 + 2 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \ldots, p_r$. Let p be any prime factor of N, so $-2 \equiv \square \bmod p$. Therefore, since $p \neq 2$, the conjecture about when $-2 \equiv \square \bmod p$ says

$p \equiv 1$ or $3 \bmod 8$. We want to show N has a prime factor which is $3 \bmod 8$, and will show this by contradiction. If every prime factor of N is $\equiv 1 \bmod 8$, then $N \equiv 1 \bmod 8$, but in fact $N \equiv 3 \bmod 8$ since $p_i^2 \equiv 1 \bmod 8$ for all i. Therefore some prime factor of N is not $1 \bmod 8$, so it is $3 \bmod 8$. This prime is different from $p_1, \dots, p_r$, so there are infinitely many primes $\equiv 3 \bmod 8$. □

Theorem 2.7. *There are infinitely many primes* $p \equiv 5 \bmod 8$.

Proof. One such prime is 5. If $p_1, \dots, p_r$ are primes $\equiv 5 \bmod 8$, let

$$N = (2p_1p_2 \cdots p_r)^2 + 1 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \dots, p_r$. Let p be any prime factor of N, so $-1 \equiv \square \bmod p$. Therefore, since $p \neq 2$, we have $p \equiv 1 \bmod 4$, which is the same as $p \equiv 1$ or $5 \bmod 8$. If every prime factor of N is $1 \bmod 8$, then $N \equiv 1 \bmod 8$, but in fact $N \equiv 5 \bmod 8$ since $p_i^2 \equiv 1 \bmod 8$ for all i. Therefore some prime factor of N is not $1 \bmod 8$, so it is $5 \bmod 8$. This prime is different from $p_1, \dots, p_r$, so there are infinitely many primes $\equiv 5 \bmod 8$. □

Theorem 2.8. *There are infinitely many primes* $p \equiv 7 \bmod 8$.

Proof. One such prime is 7. If $p_1, \dots, p_r$ are primes $\equiv 7 \bmod 8$, let

$$N = (p_1p_2 \cdots p_r)^2 - 2 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \dots, p_r$. Let p be a prime factor of N, so $2 \equiv \square \bmod p$. Therefore, since $p \neq 2$, the conjecture about when $2 \equiv \square \bmod p$ implies $p \equiv 1$ or $7 \bmod 8$. If every prime factor of N is $1 \bmod 8$, then $N \equiv 1 \bmod 8$, but in fact $N \equiv -1 \bmod 8$ since $p_i^2 \equiv 1 \bmod 8$. Therefore some prime factor of N is not $1 \bmod 8$, so it is $7 \bmod 8$. This prime is different from $p_1, \dots, p_r$, so there are infinitely many primes $\equiv 7 \bmod 8$. □

Theorem 2.9. *There are infinitely many primes* $p \equiv 5 \bmod 12$.

Proof. One such prime is 5. If $p_1, \dots, p_r$ are primes $\equiv 5 \bmod 12$, let

$$N = (2p_1p_2 \cdots p_r)^2 + 1 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \dots, p_r$. Let p be any prime factor of N, so $-1 \equiv \square \bmod p$. Therefore, since $p \neq 2$, we have $p \equiv 1 \bmod 4$, which is the same as $p \equiv 1$ or $5 \bmod 12$. (The choice $p \equiv 9 \bmod 12$ is satisfied by no prime.) If every prime factor of N is $1 \bmod 12$, then $N \equiv 1 \bmod 12$, but in fact $N \equiv 5 \bmod 12$ since $p_i^2 \equiv 1 \bmod 12$ for all i. Therefore some prime factor of N is not $1 \bmod 12$, so it is $5 \bmod 12$. This prime is different from $p_1, \dots, p_r$, so there are infinitely many primes $\equiv 5 \bmod 12$. □

Theorem 2.10. *There are infinitely many primes* $p \equiv 7 \bmod 12$.

Proof. One such prime is 7. If $p_1, \dots, p_r$ are primes $\equiv 7 \bmod 12$, let

$$N = (2p_1 \cdots p_r)^2 + 3.$$

Then N is not divisible by 2 or by any of $p_1, \dots, p_r$. Let p be any prime factor of N, so $-3 \equiv \square \bmod p$. Therefore, since p is not 2 or 3, the conjecture about when $-3 \equiv \square \bmod p$ implies $p \equiv 1 \bmod 3$. Lifting this mod 3 congruence to modulus 12 tells us $p \equiv 1, 4, 7$ or $10 \bmod 12$. There are no primes which are $4 \bmod 12$ or $10 \bmod 12$, so $p \equiv 1$ or $7 \bmod 12$. If every prime factor of N is $\equiv 1 \bmod 12$, then $N \equiv 1 \bmod 12$, but in fact $N \equiv 7 \bmod 12$ since

$p_i^2 \equiv 1 \bmod 12$ for all i (so $N \equiv 4 + 3 \bmod 12$). Therefore some prime factor of N is not $1 \bmod 12$, so it is $7 \bmod 12$. This prime is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 7 \bmod 12$. □

Theorem 2.11. *There are infinitely many primes $p \equiv 11 \bmod 12$.*

Proof. One such prime is 11. If $p_1, \ldots, p_r$ are primes $\equiv 11 \bmod 12$, let

$$N = 3(p_1 p_2 \cdots p_r)^2 - 4 > 1.$$

Then N is not divisible by 2, 3, or any of $p_1, \ldots, p_r$. Let p be a prime factor of N, so $3 \equiv \square \bmod p$ (why?). Therefore, since $p \neq 2$ or 3, the conjecture about when $3 \equiv \square \bmod p$ implies $p \equiv 1$ or $11 \bmod 12$. If every prime factor of N is $1 \bmod 12$, then $N \equiv 1 \bmod 12$, but in fact $N \equiv -1 \bmod 12$ since $p_i^2 \equiv 1 \bmod 12$ for all i. Therefore some prime factor of N is not $1 \bmod 12$, so it is $11 \bmod 12$. This prime is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 11 \bmod 12$. □

In all these proofs, we used a polynomial whose values on integers have special congruence conditions on their prime factors, *e.g.*, to show $p \equiv 4 \bmod 5$ infinitely often we relied on the fact that any integer of the form $n^2 - 5$ with n even and $n \not\equiv 0 \bmod 5$ is only divisible by primes $p \equiv 1, 4 \bmod 5$. (When $p | (n^2 - 5)$, $5 \bmod p$ is a square and $p \neq 2, 5$.) Here is a summary of the polynomial and the square condition used for each progression above.

Progression	Polynomial	Square condition
1 mod 3	$T^2 + 3$	$-3 \equiv \square \bmod p$
2 mod 3	$T - 1$	None
1 mod 4	$T^2 + 1$	$-1 \equiv \square \bmod p$
3 mod 4	$T - 1$	None
4 mod 5	$T^2 - 5$	$5 \equiv \square \bmod p$
3 mod 8	$T^2 + 2$	$-2 \equiv \square \bmod p$
5 mod 8	$T^2 + 1$	$-1 \equiv \square \bmod p$
7 mod 8	$T^2 - 2$	$2 \equiv \square \bmod p$
5 mod 12	$T^2 + 1$	$-1 \equiv \square \bmod p$
7 mod 12	$T^2 + 3$	$-3 \equiv \square \bmod p$
11 mod 12	$3T^2 - 4$	$3 \equiv \square \bmod p$

Euclid's proof of the infinitude of the primes is associated to the linear polynomial $T + 1$. (Recall the role of $p_1 \cdots p_r + 1$ in that proof.) The proofs using square patterns are those which involve a quadratic polynomial.

So far we have complete results for moduli 3 and 4, but cases remain for moduli 5, 8, and 12. For instance, are there infinitely many primes $p \equiv 2 \bmod 5$? This is not settled above.

3. Extending Euclid beyond square patterns

To prove the infinitude of primes in additional congruence classes modulo 5, 8, and 12 (such $\equiv 1 \bmod 5$, $\equiv 1 \bmod 8$, and $\equiv 1 \bmod 12$), we will use new polynomials, of degree *greater than* 2, and also use properties of orders of units in modular arithmetic. The key is to use factors of the polynomial $T^n - 1$. Here is a table of the factors for some small n.

n	$T^n - 1$
2	$T-1$
3	$(T-1)(T^2+T+1)$
4	$(T-1)(T+1)(T^2+1)$
5	$(T-1)(T^4+T^3+T^2+T+1)$
6	$(T-1)(T+1)(T^2+T+1)(T^2-T+1)$
8	$(T-1)(T+1)(T^2+1)(T^4+1)$
12	$(T-1)(T+1)(T^2+T+1)(T^2+1)(T^2-T+1)(T^4-T^2+1)$

Theorem 3.1. *There are infinitely many primes $p \equiv 1 \bmod 5$.*

Proof. We will use a factor of T^5-1: $T^4+T^3+T^2+T+1$. One prime $p \equiv 1 \bmod 5$ is 11. If $p_1, \ldots, p_r$ are primes $\equiv 1 \bmod 5$, let $n = 5p_1 \cdots p_r$ and

$$N = n^4+n^3+n^2+n+1 > 1.$$

Then N is not divisible by 5 or any of $p_1, \ldots, p_r$. Let p be a prime factor of N, so $n^4+n^3+n^2+n+1 \equiv 0 \bmod p$. Multiplying both sides by $n-1$, we get $n^5 \equiv 1 \bmod p$. Therefore $n \bmod p$ has order 1 or 5. We will show $n \bmod p$ has order 5 by contradiction. If the order is 1 then $n \equiv 1 \bmod p$, so $N \equiv 5 \bmod p$. Since $p|N$ we get $p|5$, so $p = 5$. But $p|N$ and 5 does not divide N (because 5 divides n). Therefore $p \neq 5$, which shows $n \bmod p$ doesn't have order 1 after all. Therefore the order of $n \bmod p$ is 5, so $5|(p-1)$, so $p \equiv 1 \bmod 5$. Since p is different from $p_1, \ldots, p_r$, we see there are infinitely many primes $\equiv 1 \bmod 5$. □

Theorem 3.2. *There are infinitely many primes $p \equiv 1 \bmod 8$.*

Proof. Will use a factor of T^8-1 which is not a factor of T^4-1: T^4+1.

One prime $p \equiv 1 \bmod 8$ is 17. If $p_1, \ldots, p_r$ are primes $\equiv 1 \bmod 8$, let $n = 2p_1 \cdots p_r$ and

$$N = n^4+1 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \ldots, p_r$. Let p be a prime factor of N, so $n^4 \equiv -1 \bmod p$. Then $n^8 \equiv 1 \bmod p$, so $n \bmod p$ has order dividing 8. The order can't be a proper factor of 8, since $n^4 \not\equiv 1 \bmod p$. Thus $n \bmod p$ has order 8. Since there is a non-zero number modulo p with order 8, we must have $8|(p-1)$, so $p \equiv 1 \bmod 8$. Since p is different from $p_1, \ldots, p_r$, there are infinitely many primes $\equiv 1 \bmod 8$. □

Theorem 3.3. *There are infinitely many primes $p \equiv 1 \bmod 12$.*

Proof. We will use T^4-T^2+1, which is a factor of $T^{12}-1$ but not of T^d-1 for any proper factor d of 12.

One prime $p \equiv 1 \bmod 12$ is 13. If $p_1, \ldots, p_r$ are primes $\equiv 1 \bmod 12$, let $n = 6p_1 \cdots p_r$ and set

$$N = n^4-n^2+1 > 1.$$

Then N is not divisible by 2, 3, or by any of $p_1, \ldots, p_r$. Let p be a prime factor of N, so $n^4-n^2+1 \equiv 0 \bmod p$. We now show $n \bmod p$ has order 12, which implies $12|(p-1)$, or $p \equiv 1 \bmod 12$ (and thus there are infinitely many primes $\equiv 1 \bmod 12$).

Since $n^4-n^2+1 \equiv 0 \bmod p$, we have $n^4 \equiv n^2-1 \bmod p$. Therefore $n^6 \equiv n^4-n^2 \equiv -1 \bmod p$, so $n^{12} \equiv 1 \bmod p$. Thus the order of $n \bmod p$ divides 12. If the order is not 12, then it divides 4 or 6. We already saw $n^6 \not\equiv 1 \bmod p$. If $n^4 \equiv 1 \bmod p$ then the congruence $n^4-n^2+1 \equiv 0 \bmod p$ says $2 \equiv n^2 \bmod p$. Squaring both sides, $4 \equiv 1 \bmod p$, so $p = 3$. This is not possible by the choice of n, since $3|n$ (so $n^4 \equiv 0 \bmod 3$). Therefore $n \bmod p$ has order 12 and we can apply the idea at the end of the first paragraph to complete the proof. □

A hard theorem of Dirichlet (1837) says when $(a, m) = 1$ there are infinitely many primes $p \equiv a \bmod m$. For which $a \bmod m$ can Dirichlet's theorem be proved in the style of Euclid's proof of the infinitude of the primes, as in this handout? If "style of Euclid's proof" is made precise, it turns out to be possible if and only if $a^2 \equiv 1 \bmod m$. This was proved in one direction by Schur (1901) and in the other direction by Ram Murty (1988).

For instance, there are infinitely many primes $p \equiv 2 \bmod 5$ (the first few are 2, 7, 17, 37, and 47), but since $2^2 \not\equiv 1 \bmod 5$, there is no Euclid-style proof of this result. The methods used in this handout provably can't be extended to cover the case of 2 mod 5!