Infinitely many primes which are k mod n

The problem

Are there infinitely many primes which are k mod n?

And more precise results, related to the Prime Number Theorem, led to the development of analytic number theory, beyond the scope of this course. But some cases of the problem can be dealt with by methods we have studied. We have already seen one example of the use of quadratic reciprocity. Some other cases can be dealt with in this way. See problem sheet 10 for one example.

Some cases can be dealt with even more simply.

Example

We saw that there are infinitely many primes which are 1 mod 4. Of course there are no primes which are 0 mod 4 and just one (2) which is 2 mod 4. But what about 3 mod 4?

This can be proved just using modulo arithmetic.

Suppose there are just finitely many primes q_k, $1 \le k \le n$, which are 3 mod 4. Put $N = \prod_{k=1}^{n} q_k$.

Consider N^2+2. $N^2 \equiv 1 \bmod 4$ because $q_k^2 \equiv 1 \bmod 4$ $\forall k$.

So $N^2+2 \equiv 3 \bmod 4$.

Every prime dividing N^2+2 is odd, so 1 or 3 mod 4.

At least one prime p dividing N^2+2 must be 3 mod 4

because otherwise $N^2+2 \equiv 1 \bmod 4$.

$q_k \mid N^2 \Rightarrow q_k \nmid N^2+2$ for any k, $1 \le k \le n$.

So $p \neq q_k$ for any $1 \le k \le n$. ✗

Other examples can be studied using cyclotomic polynomials

I learnt this from the webpage of Noam Elkies (lectures at Harvard)

Penelthod gives infinitely many primes which are $1 \bmod n$ using the n^{th} cyclotomic polynomial $\Phi_n(x)$ $n \geq 2$

Example There are infinitely many primes which are $1 \bmod 5$.

For this we consider $\Phi_5(x)$

$$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$$

$$\Phi_5(x) = x^4+x^3+x^2+x+1$$

Suppose there are only finitely many primes q_k $1 \leq k \leq n$ which are $\equiv 1 \bmod 5$

Put $N = \prod_{k=1}^{n} q_k$

Consider $\Phi_5(5N)$

Let p be any prime dividing $\Phi_5(5N)$

$\Phi_5(5N) \equiv 0 \bmod p$.

$p \neq q_k$ for any k because $\Phi_5(q_k)\,\Phi_5(5N) \equiv 1 \bmod q_k$

$\Phi_5(5N) \equiv 0 \overset{\bmod p}{\Rightarrow} (5N)^5 \equiv 1 \bmod p$ because $x^5 - 1 = (x-1)(\Phi_5(x))$

So $5N$ has order 1 or 5 mod p. If $5N$ has order 1 mod p

Then $5N \equiv 1 \bmod p \Rightarrow 5N \equiv 1+1+1+1+1 \equiv 5 \bmod p \Rightarrow p = 5$

But $\Phi_5(5N) \equiv 1 \bmod 5$ So $p \neq 5$

So $5N$ has order 5 mod p. Fermat's Little Theorem $\Rightarrow 5 \mid p-1$

Hence $p \equiv 1 \bmod 5$

Harder example

There are infinitely many primes which are $1 \bmod 12$

Suppose not, that there are only finitely many such primes q_k, $1 \le k \le n$.

Put $N = 6 \prod_{k=1}^{n} q_k$

Let Ψ_k denote the k-th cyclotomic polynomial

and let p be any prime dividing $\Psi_{12}(N)$

For any $k \in \mathbb{Z}_+$ $\quad x^k - 1 = \prod_{j \mid k} \Psi_j(x)$

In particular $x^{12} - 1 = \Psi_{12}(x) \times \Psi_6(x) \times \Psi_4(x) \times \Psi_3(x) \times \Psi_2(x) \times \Psi_1(x)$

$\Psi_{12}(x) \cdot x^{12} - 1 = (x^6 - 1)(x^6 + 1) = (x^6 - 1)\underbrace{(x^2 + 1)}_{\Psi_4(x)}\underbrace{(x^4 - x^2 + 1)}_{\Psi_{12}(x)}$

Claim: if $p \mid \Psi_{12}(N)$ then $p \equiv 1 \bmod 12$

This gives a contradiction because $q_k \mid N$ and so $\Psi_{12}(N) \equiv 1 \bmod q_k$

But $\Psi_{12}(N) \equiv 0 \bmod p$

Because $6 \mid N$ we also have $\Psi_{12}(N) \equiv 1 \bmod 6$

Proof of claim

$\Psi_{12}(N) \equiv 0 \bmod p \implies N^{12} - 1 \equiv 0 \bmod p$ since

$\Psi_{12}(x) \mid x^{12} - 1$. So $N^{12} \equiv 1 \bmod p$. So the order of

$N \bmod p$ is a divisor of 12, that is, 1, 2, 3, 4, 6 or 12.

We want to show N has order 12 mod p because then by Fermat's Little Theorem ($N^{p-1} \equiv 1 \bmod p$) we have $12 \mid p-1$, that is $p \equiv 1 \bmod 12$

Suppose N has order 1, 2, 3, 4 or 6.

Then $N^k \equiv 1 \bmod p$ $\quad k = 1, 2, 3, 4$ or 6.

$$N^k - 1 = \prod_{j \mid k} \Phi_j(N)$$

So $\Phi_j(N) \equiv 0 \bmod p$ for some $j = 1, 2, 3, 4$ or 6.

So $x - N$ divides $\Phi_j(x)$ in $\mathbb{Z}_p(x)$

But $x - N$ also divides $\Phi_{12}(x)$ in $\mathbb{Z}_p(x)$.

So $x^{12} - 1 = (x-N)^2 f(x)$ for some $f(x) \in \mathbb{Z}_p[x]$.

So $12x^{11} \equiv (x-N)^2 f'(x) + 2(x-N)f(x)$ in $\mathbb{Z}_p[x]$

So $12N^{11} \equiv 0 \bmod p$.

$p \equiv 1 \bmod 6$ So 12 is coprime to p (because 2, 3 coprime to p)

So $N^{11} \equiv 0 \bmod p$ and $N \equiv 0 \bmod p$

But But then $\Phi_{12}(N) \equiv 1 \bmod p$ - ✗.