Number Theory Section Summary: 3.3

The Goldbach Conjecture

1. Summary

We now can prove that the primes are infinite in number, and we have no doubt sensed the feeling that their distribution is uneven (since so many appear in the first 10 natural numbers, and then start to get annihilated in the spiraling patterns of the sieve of Eratosthenes). But what can we say about the distribution of primes? Are there interesting patterns? This section seeks to sum up some of what we know.

Various famous interesting conundrums, mysteries, conjectures, etc. are discussed, including

- The Goldbach Conjecture;
- Twin Primes, and other gaps between primes;
- Dirichlet's theorem about primes of the form $a+kb$, with $\gcd(a,b) = 1$;
- Primes of various forms given by the division algorithm;

2. Definitions

Twin primes: prime pairs of the form p, $p+2$.

Euler polynomial: $f(n) = n^2 + n + 41$ (which produces primes for the integers from 0 to 39).

3. Theorems

Goldbach Conjecture: Every even $n > 2$ is the sum of two primes.

Note: it's interesting that it's been shown (Vinogradov) that

$$\lim_{x\to\infty} \frac{A(x)}{x} = 0$$

where $A(x)$ is the number of evens less than or equal to x and not expressible as the sum of two primes. ($A(x)$ may be zero for all x!) This means that "almost all" integers satisfy the conjecture. *What does that mean?!*

Twin Prime Conjecture: There are infinitely many twin primes.

Lemma: The product of two or more integers of the form $4n+1$ is of the same form.

Theorem 3.6: There are an infinite number of primes of the form $4n+3$.

Example: Exercise #13, p. 60 asks us to show the same thing for integers of the form $6n+5$.

Theorem 3.7 (Dirichlet): If a and b are relatively prime positive integers, then the arithmetic progression

$$a,\ a+b,\ a+2b,\ a+3b,\ldots$$

contains infinitely many primes.

Theorem 3.8: If all the $n>2$ terms of the arithmetic progression

$$p,\ p+d,\ p+2d,\ \ldots,p+(n-1)d$$

are prime numbers, then the common difference d is divisible by every prime $q<n$.

4. Properties/Tricks/Hints/Etc.

#13 p 60. There are infinitely many primes of the form $6n+5$.

Lemma: The product of integers of the form $6n+1$ is an integer of form $6n+1$

Given $a = 6n+1$ & $b = 6m+1$.

$$a \cdot b = (6n+1)(6m+1)$$
$$= 36nm + 6n + 6m + 1$$
$$= 6[6nm + n + m] + 1$$ ✓

By contradiction: suppose there are only finitely many such primes, $q_1, \ldots, q_r$.

Consider

$$N = 6q_1 \cdots q_r - 1 \quad \Rightarrow \quad 1 = 6q_1 \cdots q_r - N$$
$$= 6[q_1 \cdots q_r - 1] + 5$$

$N = p_1^{k_1} \cdots p_s^{k_s}$ (N has a prime factorization).

N is of the form $6z+5$, so one of its prime factors $p_i = q_j$. So $q_j \mid N$ – oops! $\gcd(q_j, N) = 1$! Contradiction.

#20, p60

If p & p^2+8 are both prime, prove that p^3+4 is also prime.

If p is prime & other than 2 or 3, then

① $p = 6n+1$ or ② $p = 6n+5$

① $p^2+8 = (6n+1)^2+8$

$= 36n^2+12n+9$ divisible by 3 (not prime!)

② $p^2+8 = (6n+5)^2+8$

also divisible by 3, & not prime

True! But its only useful in the case $p=3$.

#23 $\frac{5+7}{2} = \underbrace{6 = \frac{3 \cdot 4}{2}}_{\text{triangular}}$

$$\frac{p+(p+2)}{2} = \frac{n(n+1)}{2}$$

$$2p+2 = n(n+1)$$

$$2p = n^2+n-2 = (n+2)(n-1)$$

Either:

$$\underbrace{\begin{array}{l} 2 = n+2 \\ p = n-1 \end{array}}$$

$\Rightarrow$ $p = -1$

False!

or:

$$\underbrace{\begin{array}{l} 2 = n-1 \\ p = n+2 \end{array}}$$

$n = 3$

$p = 5$

b) is similar

or:

$$\left.\begin{array}{l} n+2 = 1 \\ n-1 = 2p \end{array}\right\} \Rightarrow$$

$n = -1$, $p < 0$ False!

or: $\left.\begin{array}{l} n-1 = 1 \\ n+2 = 2p \end{array}\right\}$ $\begin{array}{l} n = 2 \\ p = 2 \end{array}$

$p + 2 = 4$, not prime!

False