

$$(1|p) = +1$$

$$(n|p) = -1$$

$$(nm|p) = (n|p)(m|p)$$


$$res \times res = res$$

$$n.res \times n.res = res$$

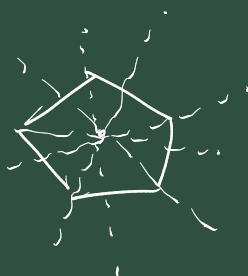
$$n.res \times res = n.res.$$

$$(p|q) = \begin{cases} -(q|p), & q \equiv p \equiv 3 \pmod{4} \\ (q|p), & \text{otherwise.} \end{cases}$$

$D_n$  = group of symmetries of  $n$ -sided regular polygon.

eg.  $D_3$  

$D_4$  

$D_5$  

$$D_n = \langle r, s \rangle, \quad r^n = e, \quad s^2 = e$$

$$sr = r^{-1}s \quad |D_n| = 2n$$

$$\text{So } D_n = \{ e, r, r^2, r^3, \dots, r^{n-1}, \\ s, rs, r^2s, r^3s, \dots, r^{n-1}s \}$$

There is the subgroup

$$R = \{ e, r, r^2, r^3, \dots, r^{n-1} \}$$

$R$  is a subgroup of  $D_n$ .  $|R| = n$ .

$$R = \langle r \rangle$$

Now in general  $R$  itself will have subgroups which will also be subgroups of  $D_n$ .

There is also the subgroup

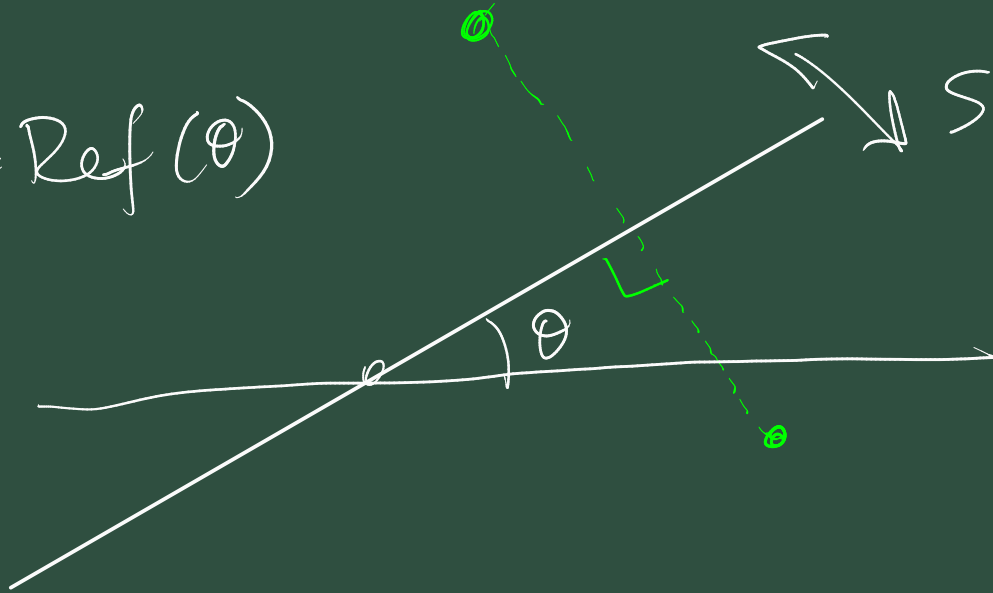
$$\langle s \rangle = \{ e, s \} \cap D_n.$$

and other subgroups containing reflections too.  $|\langle s \rangle| = 2$

---

$$e \cdot e = e$$

$$S = \text{Ref}(\theta)$$



$$S^2 = e$$

$$S.S = e.$$

For a reflection  $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$   
can represent it with a  
reflection matrix

$$S = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

can show  $S^{-1} = S$

$S^2 = \text{identity matrix.}$

$$S.S = I \Rightarrow S = S^{-1}$$

Recall: there are an infinite number  
of primes.

How are they distributed in  $\mathbb{Z}$ .

think of  $\mathbb{Z}$  modulo 4.

any integer  $z \equiv 0, 1, 2, 3 \pmod{4}$

If  $p$  is an odd prime

$$p \equiv 1, 3 \pmod{4}$$

3, 5, 7, 11, 13, 17, 19, 23, ...

3 1 3 3 1 1 3 3, ...

in fact there are an infinite  
number of primes  $\equiv 1 \pmod{4}$   
 $\equiv 3 \pmod{4}$ .

in fact there is a general  
result Dirichlet's Theorem which  
says if  $\gcd(a, n) = 1$

then there is an infinite number of primes  $\equiv a \pmod{n}$ .

We can prove some special cases of Dirichlet's theorem (i.e. for certain  $a, n$ )

Ex 8.5 Q3 (a).

Claim: there are an infinite number of primes  $p$  of the form  $p = 4n - 1$ .

Proof By contradiction.

Assume there's only a finite number of primes  $p = 4n - 1$ .

Then let  $\underline{P}$  be the largest one.

Then consider the integer  $N$ .

$$N = (2^2 \times 3 \times 5 \times 7 \times \dots \times \underline{P}) - 1$$

product of all the primes from 3 to  $\underline{P}$ .

we know  $N$  has prime factors  $q$

note that  $q > \underline{P}$ .

because if  $q \leq \underline{P}$  then  $q$  is  
in this factor  $2 \times 3 \times \dots \times \underline{P}$

in which case  $q \mid N$

and  $q \mid (2^2 \times 3 \times \dots \times \underline{P})$

~~and~~ and so  $q \mid 1$ .

since  $1 = -N + (2^2 \times 3 \times 5 \times \dots \times \underline{P})$ .

which is a contradiction.

so all prime factors  $q$  of  $N$  are  
satisfying  $q > \underline{P}$ .

so all these  $q$  must have

the form  $4n+1$  for ~~various~~

various  $n$ , i.e.  $q \equiv 1 \pmod{4}$

$$\Rightarrow N \equiv 1 \pmod{4}$$

as  $N$  is the product of all its  
prime divisors.

But this contradicts the definition of  $N$

as

$$N = 4 \times (3 \times \dots \times P) - 1.$$

$$\equiv 3 \pmod{4}$$

So we've got a contradiction.

So we conclude there is no largest

prime  $P$  of the form  $4n-1$ , so

there is an infinite number of them.

(b). There are an infinite number  
of primes of the form  $p = 8k+3$ .

3, 5, 7, 11, 13, 17, 19, 23, , 29, 31, 37, 41, 43, 47, 53, 59, 67, 71, 79, 83, 89, 97, 101, 103, 107, 113, 127, 131, 137, 149, 151, 157, 163, 167, 173, 179, 181, 187, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 527, 529, 533, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 623, 629, 631, 637, 641, 643, 647, 653, 659, 661, 667, 671, 673, 677, 683, 689, 691, 697, 701, 703, 707, 709, 713, 719, 727, 729, 731, 733, 737, 739, 743, 749, 751, 757, 761, 763, 767, 769, 773, 779, 781, 787, 791, 793, 797, 799, 803, 809, 811, 817, 821, 823, 827, 829, 833, 837, 839, 841, 847, 851, 853, 857, 859, 863, 867, 869, 871, 877, 881, 883, 887, 891, 893, 897, 899, 901, 903, 907, 909, 911, 913, 917, 919, 923, 927, 929, 931, 933, 937, 939, 941, 943, 947, 949, 951, 953, 957, 959, 961, 963, 967, 969, 971, 973, 977, 979, 981, 983, 987, 989, 991, 993, 997, 999, 1000, 1001, 1003, 1007, 1009, 1013, 1017, 1019, 1021, 1023, 1027, 1029, 1031, 1033, 1037, 1039, 1041, 1043, 1047, 1049, 1051, 1053, 1057, 1059, 1061, 1063, 1067, 1069, 1071, 1073, 1077, 1079, 1081, 1083, 1087, 1089, 1091, 1093, 1097, 1099, 1101, 1103, 1107, 1109, 1111, 1113, 1117, 1119, 1121, 1123, 1127, 1129, 1131, 1133, 1137, 1139, 1141, 1143, 1147, 1149, 1151, 1153, 1157, 1159, 1161, 1163, 1167, 1169, 1171, 1173, 1177, 1179, 1181, 1183, 1187, 1189, 1191, 1193, 1197, 1199, 1201, 1203, 1207, 1209, 1211, 1213, 1217, 1219, 1221, 1223, 1227, 1229, 1231, 1233, 1237, 1239, 1241, 1243, 1247, 1249, 1251, 1253, 1257, 1259, 1261, 1263, 1267, 1269, 1271, 1273, 1277, 1279, 1281, 1283, 1287, 1289, 1291, 1293, 1297, 1299, 1301, 1303, 1307, 1309, 1311, 1313, 1317, 1319, 1321, 1323, 1327, 1329, 1331, 1333, 1337, 1339, 1341, 1343, 1347, 1349, 1351, 1353, 1357, 1359, 1361, 1363, 1367, 1369, 1371, 1373, 1377, 1379, 1381, 1383, 1387, 1389, 1391, 1393, 1397, 1399, 1401, 1403, 1407, 1409, 1411, 1413, 1417, 1419, 1421, 1423, 1427, 1429, 1431, 1433, 1437, 1439, 1441, 1443, 1447, 1449, 1451, 1453, 1457, 1459, 1461, 1463, 1467, 1469, 1471, 1473, 1477, 1479, 1481, 1483, 1487, 1489, 1491, 1493, 1497, 1499, 1501, 1503, 1507, 1509, 1511, 1513, 1517, 1519, 1521, 1523, 1527, 1529, 1531, 1533, 1537, 1539, 1541, 1543, 1547, 1549, 1551, 1553, 1557, 1559, 1561, 1563, 1567, 1569, 1571, 1573, 1577, 1579, 1581, 1583, 1587, 1589, 1591, 1593, 1597, 1599, 1601, 1603, 1607, 1609, 1611, 1613, 1617, 1619, 1621, 1623, 1627, 1629, 1631, 1633, 1637, 1639, 1641, 1643, 1647, 1649, 1651, 1653, 1657, 1659, 1661, 1663, 1667, 1669, 1671, 1673, 1677, 1679, 1681, 1683, 1687, 1689, 1691, 1693, 1697, 1699, 1701, 1703, 1707, 1709, 1711, 1713, 1717, 1719, 1721, 1723, 1727, 1729, 1731, 1733, 1737, 1739, 1741, 1743, 1747, 1749, 1751, 1753, 1757, 1759, 1761, 1763, 1767, 1769, 1771, 1773, 1777, 1779, 1781, 1783, 1787, 1789, 1791, 1793, 1797, 1799, 1801, 1803, 1807, 1809, 1811, 1813, 1817, 1819, 1821, 1823, 1827, 1829, 1831, 1833, 1837, 1839, 1841, 1843, 1847, 1849, 1851, 1853, 1857, 1859, 1861, 1863, 1867, 1869, 1871, 1873, 1877, 1879, 1881, 1883, 1887, 1889, 1891, 1893, 1897, 1899, 1901, 1903, 1907, 1909, 1911, 1913, 1917, 1919, 1921, 1923, 1927, 1929, 1931, 1933, 1937, 1939, 1941, 1943, 1947, 1949, 1951, 1953, 1957, 1959, 1961, 1963, 1967, 1969, 1971, 1973, 1977, 1979, 1981, 1983, 1987, 1989, 1991, 1993, 1997, 1999, 2001, 2003, 2007, 2009, 2011, 2013, 2017, 2019, 2021, 2023, 2027, 2029, 2031, 2033, 2037, 2039, 2041, 2043, 2047, 2049, 2051, 2053, 2057, 2059, 2061, 2063, 2067, 2069, 2071, 2073, 2077, 2079, 2081, 2083, 2087, 2089, 2091, 2093, 2097, 2099, 2101, 2103, 2107, 2109, 2111, 2113, 2117, 2119, 2121, 2123, 2127, 2129, 2131, 2133, 2137, 2139, 2141, 2143, 2147, 2149, 2151, 2153, 2157, 2159, 2161, 2163, 2167, 2169, 2171, 2173, 2177, 2179, 2181, 2183, 2187, 2189, 2191, 2193, 2197, 2199, 2201, 2203, 2207, 2209, 2211, 2213, 2217, 2219, 2221, 2223, 2227, 2229, 2231, 2233, 2237, 2239, 2241, 2243, 2247, 2249, 2251, 2253, 2257, 2259, 2261, 2263, 2267, 2269, 2271, 2273, 2277, 2279, 2281, 2283, 2287, 2289, 2291, 2293, 2297, 2299, 2301, 2303, 2307, 2309, 2311, 2313, 2317, 2319, 2321, 2323, 2327, 2329, 2331, 2333, 2337, 2339, 2341, 2343, 2347, 2349, 2351, 2353, 2357, 2359, 2361, 2363, 2367, 2369, 2371, 2373, 2377, 2379, 2381, 2383, 2387, 2389, 2391, 2393, 2397, 2399, 2401, 2403, 2407, 2409, 2411, 2413, 2417, 2419, 2421, 2423, 2427, 2429, 2431, 2433, 2437, 2439, 2441, 2443, 2447, 2449, 2451, 2453, 2457, 2459, 2461, 2463, 2467, 2469, 2471, 2473, 2477, 2479, 2481, 2483, 2487, 2489, 2491, 2493, 2497, 2499, 2501, 2503, 2507, 2509, 2511, 2513, 2517, 2519, 2521, 2523, 2527, 2529, 2531, 2533, 2537, 2539, 2541, 2543, 2547, 2549, 2551, 2553, 2557, 2559, 2561, 2563, 2567, 2569, 2571, 2573, 2577, 2579, 2581, 2583, 2587, 2589, 2591, 2593, 2597, 2599, 2601, 2603, 2607, 2609, 2611, 2613, 2617, 2619, 2621, 2623, 2627, 2629, 2631, 2633, 2637, 2639, 2641, 2643, 2647, 2649, 2651, 2653, 2657, 2659, 2661, 2663, 2667, 2669, 2671, 2673, 2677, 2679, 2681, 2683, 2687, 2689, 2691, 2693, 2697, 2699, 2701, 2703, 2707, 2709, 2711, 2713, 2717, 2719, 2721, 2723, 2727, 2729, 2731, 2733, 2737, 2739, 2741, 2743, 2747, 2749, 2751, 2753, 2757, 2759, 2761, 2763, 2767, 2769, 2771, 2773, 2777, 2779, 2781, 2783, 2787, 2789, 2791, 2793, 2797, 2799, 2801, 2803, 2807, 2809, 2811, 2813, 2817, 2819, 2821, 2823, 2827, 2829, 2831, 2833, 2837, 2839, 2841, 2843, 2847, 2849, 2851, 2853, 2857, 2859, 2861, 2863, 2867, 2869, 2871, 2873, 2877, 2879, 2881, 2883, 2887, 2889, 2891, 2893, 2897, 2899, 2901, 2903, 2907, 2909, 2911, 2913, 2917, 2919, 2921, 2923, 2927, 2929, 2931, 2933, 2937, 2939, 2941, 2943, 2947, 2949, 2951, 2953, 2957, 2959, 2961, 2963, 2967, 2969, 2971, 2973, 2977, 2979, 2981, 2983, 2987, 2989, 2991, 2993, 2997, 2999, 3001, 3003, 3007, 3009, 3011, 3013, 3017, 3019, 3021, 3023, 3027, 3029, 3031, 3033, 3037, 3039, 3041, 3043, 3047, 3049, 3051, 3053, 3057, 3059, 3061, 3063, 3067, 3069, 3071, 3073, 3077, 3079, 3081, 3083, 3087, 3089, 3091, 3093, 3097, 3099, 3101, 3103, 3107, 3109, 3111, 3113, 3117, 3119, 3121, 3123, 3127, 3129, 3131, 3133, 3137, 3139, 3141, 3143, 3147, 3149, 3151, 3153, 3157, 3159, 3161, 3163, 3167, 3169, 3171, 3173, 3177, 3179, 3181, 3183, 3187, 3189, 3191, 3193, 3197, 3199, 3201, 3203, 3207, 3209, 3211, 3213, 3217, 3219, 3221, 3223, 3227, 3229, 3231, 3233, 3237, 3239, 3241, 3243, 3247, 3249, 3251, 3253, 3257, 3259, 3261, 3263, 3267, 3269, 3271, 3273, 3277, 3279, 3281, 3283, 3287, 3289, 3291, 3293, 3297, 3299, 3301, 3303, 3307, 3309, 3311, 3313, 3317, 3319, 3321, 3323, 3327, 3329, 3331, 3333, 3337, 3339, 3341, 3343, 3347, 3349, 3351, 3353, 3357, 3359, 3361, 3363, 3367, 3369, 3371, 3373, 3377, 3379, 3381, 3383, 3387, 3389, 3391, 3393, 3397, 3399, 3401, 3403, 3407, 3409, 3411, 3413, 3417, 3419, 3421, 3423, 3427, 3429, 3431, 3433, 3437, 3439, 3441, 3443, 3447, 3449, 3451, 3453, 3457, 3459, 3461, 3463, 3467, 3469, 3471, 3473, 3477, 3479, 3481, 3483, 3487, 3489, 3491, 3493, 3497, 3499, 3501, 3503, 3507, 3509, 3511, 3513, 3517, 3519, 3521, 3523, 3527, 3529, 3531, 3533, 3537, 3539, 3541, 3543, 3547, 3549, 3551, 3553, 3557, 3559, 3561, 3563, 3567, 3569, 3571, 3573, 3577, 3579, 3581, 3583, 3587, 3589, 3591, 3593, 3597, 3599, 3601, 3603, 3607, 3609, 3611, 3613, 3617, 3619, 3621, 3623, 3627, 3629, 3631, 3633, 3637, 3639, 3641, 3643, 3647, 3649, 3651, 3653, 3657, 3659, 3661, 3663, 3667, 3669, 3671, 3673, 3677, 3679, 3681, 3683, 3687, 3689, 3691, 3693, 3697, 3699, 3701, 3703, 3707, 3709, 3711, 3713, 3717, 3719, 3721, 3723, 3727, 3729, 3731, 3733, 3737, 3739, 3741, 3743, 3747, 3749, 3751, 3753, 3757, 3759, 3761, 3763, 3767, 3769, 3771, 3773, 3777, 3779, 3781, 3783, 3787, 3789, 3791, 3793, 3797, 3799, 3801, 3803, 3807, 3809, 3811, 3813, 3817, 3819, 3821, 3823, 3827, 3829, 3831, 3833, 3837, 3839, 3841, 3843, 3847, 3849, 3851, 3853, 3857, 3859, 3861, 3863, 3867, 3869, 3871, 3873, 3877, 3879, 3881, 3883, 3887, 3889, 3891, 3893, 3897, 3899, 3901, 3903, 3907, 3909, 3911, 3913, 3917, 3919, 3921, 3923, 3927, 3929, 3931, 3933, 3937, 3939, 3941, 3943, 3947, 3949, 3951, 3953, 3957, 3959, 3961, 3963, 3967, 3969, 3971, 3973, 3977, 3979, 3981, 3983, 3987, 3989, 3991, 3993, 3997, 3999, 4001, 4003, 4007, 4009, 4011, 4013, 4017, 4019, 4021, 4023, 4027, 4029, 4031, 4033, 4037, 4039, 4041, 4043, 4047, 4049, 4051, 4053, 4057, 4059, 4061, 4063, 4067, 4069, 4071, 4073, 4077, 4079, 4081, 4083, 4087, 4089, 4091, 4093, 4097, 4099, 4101, 4103, 4107, 4109, 4111, 4113, 4117, 4119, 4121, 4123, 4127, 4129, 4131, 4133, 4137, 4139, 4141, 4143, 4147, 4149, 4151, 4153, 4157, 4159, 4161, 4163, 4167, 4169, 4171, 4173, 4177, 4179, 4181, 4183, 4187, 4189, 4191, 4193, 4197, 4199, 4201, 4203, 4207, 4209, 4211, 4213, 4217, 4219, 4221, 4223, 4227, 4229, 4231, 4233, 4237, 4239, 4241, 4243, 4247, 4249, 4251, 4253, 4257, 4259, 4261, 4263, 4267, 4269, 4271, 4273, 4277, 4279, 4281, 4283, 4287, 4289, 4291, 4293, 4297, 4299, 4301, 4303, 4307, 4309, 4311, 4313, 4317, 4319, 4321, 4323, 4327, 4329, 4331, 4333, 4337, 4339, 4341, 4343, 4347, 4349, 4351, 4353, 4357, 4359, 4361, 4363, 4367, 4369, 4371, 4373, 4377, 4379, 4381, 4383, 4387, 4389, 4391, 4393, 4397, 4399, 4401, 4403, 4407, 4409, 4411, 4413, 4417, 4419, 4421, 4423, 4427, 4429, 4431, 4433, 4437, 4439, 4441, 4443, 4447, 4449, 4451, 4453, 4457, 4459, 4461, 4463, 4467, 4469, 4471, 4473, 4477, 4479, 4481, 4483, 4487, 4489, 4491, 4493, 4497, 4499, 4501, 4503, 4507, 4509, 4511, 4513, 4517, 4519, 4521, 4523, 4527, 4529, 4531, 4533, 4537, 4539, 4541, 4543, 4547, 4549, 4551, 4553, 4557, 4559, 4561, 4563, 4567, 4569, 4571, 4573, 4577, 4579, 4581, 4583, 4587, 4589, 4591, 4593, 4597, 4599, 4601, 4603, 4607, 4609, 4611, 4613, 4617, 4619, 4621, 4623, 4627, 4629, 4631, 4633, 4637, 4639, 4641, 4643, 4647, 4649, 4651, 4653, 4657, 4659, 4661, 4663, 4667, 4669, 4671, 4673, 4677, 4679, 4681, 4683, 4687, 4689, 4691, 4693, 4697, 4699, 4701, 4703, 4707, 4709, 4711, 4713, 4717, 4719, 4721, 4723, 4727, 4729, 4731, 4733, 4737, 4739, 4741, 4743, 4747, 4749, 4751, 4753, 4757, 4759, 4761, 4763, 4767, 4769, 4771, 4773, 4777, 4779, 4781, 4783, 4787, 4789, 4791, 4793, 4797, 4799, 4801, 4803, 4807, 4809, 4811, 4813, 4817, 4819, 4821, 4823, 4827, 4829, 4831, 4833, 4837, 4839, 4841, 4843, 4847, 4849, 4851, 4853, 4857, 4859, 4861, 4863, 4867, 4869, 4871, 4873, 4877, 4879, 4881, 4883, 4887, 4889, 4891, 4893, 4897, 4899, 4901, 4903, 4907, 4909, 4911, 4913, 4917, 4919, 4921, 4923, 4927, 4929, 4931, 4933, 4937, 4939, 4941, 4943, 4947, 4949, 4951, 4953, 4957, 4959, 4961, 4963, 4967, 4969, 4971, 4973, 4977, 4979, 4981, 4983, 4987, 4989, 4991, 4993, 4997, 4999, 5001, 5003, 5007, 5009, 5011, 5013, 5017, 5019, 5021, 5023, 5027, 5029, 5031, 5033, 5037, 5039, 5041, 5043, 5047, 5049, 5051, 5053, 5057, 5059, 5061, 5063, 5067, 5069, 5071, 5073, 5077, 5079, 5081, 5083, 5087, 5089, 5091, 5093, 5097, 5099, 5101, 5103, 5107, 5109, 5111, 5113, 5117, 5119, 5121, 5123, 5127, 5129, 5131, 5133, 5137, 5139, 5141, 5143, 5147, 5149, 5151, 5153, 5157, 5159, 5161, 5163, 5167, 5169, 5171, 5173, 5177, 5179, 5181, 5183, 5187, 5189, 5191, 5193, 5197, 5199, 5201, 5203, 5207, 5209, 5211, 5213, 5217, 5219, 5221, 5223, 5227, 5229, 5231, 5233, 5237, 5239, 5241, 5243, 5247, 5249, 5251, 5253, 5257, 5259, 5261, 5263, 5267, 5269, 5271, 5273, 5277, 5279, 5281, 5283, 5287, 5289, 5291, 5293, 5297, 5299, 5301, 5303, 5307, 5309, 5311, 5313, 5317, 5319, 5321, 5323, 5327, 5329, 5331, 5333, 5337, 5339, 5341, 5343, 5347, 5349, 5351, 5353, 5357, 5359, 5361, 5363, 5367, 5369, 5371, 5373, 5377, 5379, 5381, 5383, 5387, 5389, 5391, 5393, 5397, 5399, 5401, 5403, 5407, 5409, 5411, 5413, 5417, 5419, 5421, 5423, 5427, 5429, 5431, 5433, 5437, 5439, 5441, 5443, 5447, 5449, 5451, 5453, 5457, 5459, 5461, 5463, 5467, 5469, 5471, 54

Proof (by contradiction)

Assume there's only a finite number.  $P_1, \dots, P_s \equiv 3 \pmod{8}$

Then consider.

$$N = (P_1 \dots P_s)^2 + 2.$$

note  $N \equiv ? \pmod{8}$

$$N = P_1^2 P_2^2 \dots P_s^2 + 2.$$

$$\equiv 1 \cdot 1 \cdot \dots \cdot 1 + 2 \pmod{8}$$

$$\equiv 3 \pmod{8} \text{ so } N \text{ is odd.}$$

Let  $q$  be an odd prime divisor of  $N$ .

Also note that  $-2$  is a quadratic residue modulo  $N$ .

$$-2 \equiv -N + (P_1 \dots P_s)^2$$

$$-2 \equiv -mq + (P_1 \dots P_s)^2$$

$$\text{so } (-2|N) = +1. \text{ so } (-2|q) = +1$$



$$\Rightarrow (-1|q)(2|q) = +1.$$

Two cases

$$\text{either } (-1|q) = -1 \Rightarrow q \equiv 3 \pmod{4}.$$

$$\& (2|q) = -1 \Rightarrow q \equiv 3, 5 \pmod{8}.$$

OR

$$(-1|q) = +1 \Rightarrow q \equiv 1 \pmod{4}.$$

$$(2|q) = +1 \Rightarrow q \equiv 1, 7 \pmod{8}$$

Therefore  $q \equiv 1$  or  $3 \pmod{8}$

But the prime divisors  $q$  of  $N$   
cannot all  $\equiv 1 \pmod{8}$

since then  $N \equiv 1 \pmod{8}$

but this contradicts  $N \equiv 3 \pmod{8}$ .

So  $N$  must have at least one  
prime divisor  $q \equiv 3 \pmod{8}$ .

So  $q = p_i$  for some  $1 \leq i \leq s$

But we get that  $q \mid N$  and

$$q \mid (p_1 \cdots p_s)^2$$

and so  $q \mid 2$  since

$$2 = N - (p_1 \cdots p_s)^2$$

$$\Rightarrow q = 2.$$

~~This contradicts the fact that~~  
 $N$  is odd.

So there must be an infinite  
number of primes of the form  
 $\equiv 3 \pmod{8}$

Ex 8.4. Q10.  $x^2 \equiv 29 \pmod{53}$

$$(29/53) = (53/29), \text{ by Q.R.}$$

$$= (24/29), \text{ reduction}$$

$$= (2/29)^3 (3/29) \quad 53 \equiv 24 \pmod{29}$$

$$= (2/29)(3/29) \quad \text{factorization}$$

$$= -(3/29), \text{ by } (2/p)$$

$$= -(29/3) \quad \text{result and } 29 \equiv 5 \pmod{8}$$

$$= -(2/3)$$

$$= -(-1), \quad 2 \text{ is a non-residue modulo } 3.$$

$$= +1$$

So 29 is a quadratic residue modulo 53.

Q1 (c)

Consider  $5x^2 + 6x + 1 \equiv 0 \pmod{23}$

Solutions if they exist are given by

$$x = (-6 + u)(10)^{-1} \pmod{23}$$

where  $u$  is an element satisfying

$$u^2 \equiv \underbrace{6^2 - 4 \cdot 5}_{\text{discriminant.}} \pmod{23}$$

$$\equiv 36 - 20$$

$$\equiv 16 \pmod{23}$$

$$\equiv (\pm 4)^2$$

$$\text{So } u \equiv 4, 19 \pmod{23}$$

So there are two solutions.

$$\text{Note } 7 \cdot 10 = 70 \equiv 1 \pmod{23}.$$

$$\text{So } 10^{-1} \equiv 7 \pmod{23}.$$

$$\text{sols are } -6 \equiv 17 \pmod{23}.$$

$$x = (17 + 4) \cdot 7.$$

$$= 21 \cdot 7.$$

$$= 147$$

$$\equiv \underline{\underline{9}} \pmod{23}.$$

$$x \equiv (17 + 19) \cdot 7.$$

$$= (36) \cdot 7.$$

$$\equiv 13 \cdot 7 \pmod{23}.$$

$$\equiv 91$$

$$\equiv \underline{\underline{22}} \pmod{23}$$

