Martina Tomisová
mtomisova@seznam.cz

Podrobná specifikace ročníkového projektu

Analýza existujících programů

Distribuovanými výpočty prvočísel se zabývalo již mnoho projektů, vybrala jsem tři nejzajímavější:

(i) Great Internet Mersenne Prime Search (GIMPS)
www.mersenne.org
Cílem je najít prvočísla dlouhá 10 milionů cifer. Počítají pouze čísla ve tvaru 2^n-1. Výhodou je malý přenos dat mezi serverem a klientem a snažší uložení čísel do databáze (stačí pracovat s exponentem). Nevýhoda je omezený tvar prvočísla – některá tímto způsobem nenajdou.
Na webových stránkách projektu nabízejí verze klientů pro široké spektrum OS.
Na nalezeni těchto prvočísel byla vypsána odměna, tedy před používáním jejich programu je nutnou souhlasit s úmluvou o rozdělení odměny mezi autory projektu a uživatele klienta, který číslo objevil.
Tento projekt má s mým některé společné rysy:
- komunikace se serverem pomocí http protokolu
- klient běží s nejnižší prioritou
- klient si průběžně ukládá výsledky a stručně pomocí výpisu na konzoli informuje uživatele o výsledcích výpočtů

(ii) Ballinger-Keller search
http://www.glasgowg43.freeserve.co.uk/siersurv.htm
Snažili se vypočítat prvočísla ve tvaru $k^* 2^n + 1$ pro $n < 1000$ a $78557 < k < 10^6$, projekt byl již úspěšně ukončen na počátku tohoto roku (2006), výsledky jsou zveřejněny na webových stránkách projektu.

(iii) Ten Primes
http://www.ltkz.demon.co.uk/ar2/10primes.htm
Tento projekt je také již ukončen a také s úspěchem (1998). Cílem bylo naleznout 10 pročísel po sobě jdoucích v nějaké aritmetické posloupnosti. Nalezená prvočísla měla 97 cifer.

Popis všech funkcí a vlastností programu

Projekt se skládá ze dvou částí: server a klient. Serverová část bude spuštěna na jediném http serveru a bude komunikovat pomocí http protokolu s klienty, kterých bude spuštěno mnoho na mnoha nezávislých počítačích.

Lehký přehled

Kdesi na síti poběží server. Uživatel si stáhne klienta a spustí ho. Při prvním spuštění se klient dotáže na email uživatele (slouží jako login) a jeho heslo, údaje odešle a uloží si je pro příští přihlášení, server klienta zaregistruje. Při dalším spuštění se již klient zaloguje sám. Jakmile bude mít klient zadanou práci, bude počítat. Pokud ne, spojí se serverem a požádá o její přidělění. Až práci dokončí, výsledky odešle serveru. Klient poběží s nejnižší prioritou, aby uživatele neobtěžoval.
Při tomto stylu provozu mohou nastat následující zvláštní situace:

- Pokud by v okamžiku potřeby nebyl klient na síti nebo se mu z jiného důvodu nepovedlo se spojit se serverem, vygeneruje si vlastní balík práce, aby mohl počítat.
- Do projektu se mohou zapojit i osoby s nečistými úmysly a je tedy třeba odfiltrovat špatné výsledky. Server tedy bude zadávat stejnou práci více různým lidem (odliší je podle loginu a ip adresy) a výsledek označí za platný a konečný až tehdy, pokud se na něm alespoň *k* klientů, co ho počítali (tento limit bude možné nastavit v konfiguračním souboru před spuštěním serveru).

Funkce serveru

(a) velikost prvočísel a počet ověřování čísel budou pevně stanoveny před prvním spuštěním serveru v konfiguračním souboru
(b) udržování databáze (prvo)čísel
(c) databáze čísel k prozkoumání i už prozkoumaných bude MySQL databáze
(d) u každého čísla bude označeno, zda je již prozkoumané, jaký je výsledek zkoumání, kdo ho zkoumal a z jaké ip adresy se připojoval
(e) číslo bude označeno jako prozkoumané po tom, co ke stejnému výsledku došlo alespoň *k* klientů s různými loginy a z různých ip adres
(f) udržování databáze klientů
(g) každý klient bude mít svůj login (email) a heslo
(h) komunikace s klienty:

- autorizuje klienta
- ověření klienta
- registrace nového klienta
- poslání zapomenutého hesla na email (pokud je email již zaregistrován a klient se ho znovu pokusí zaregistrovat)

(i) pokud klient požádá o zadání práce, pošle mu rozmezí čísel, která má klient ověřit
(j) pokud klient doručí výsledky, uloží si je (ve formátu ANO/NE k danému číslu)

Funkce klienta

(a) při prvním spuštění (nebo při spuštění s absencí konfiguračního souboru) se zeptá uživatele na login a heslo a pokusí se ho zaregistrovat
(b) pokud klient nebude mít co počítat, pošle serveru požadavek o zadání práce, pokud se mu nepodaří se se serverem spojit, vygeneruje náhodně nové kandidáty a zkusí je ověřit
(c) pokud má klient zadánu práci, počítá
(d) pokud má výsledky, které ještě neodeslal serveru, zkusí mu je poslat po získání každé nové sady výsledků
(e) před každou komunikací se serverem se klient autentizuje pomocí loginu a hesla, které jsou uloženy v konfiguračním souboru, pokud ještě heslo a login nemá, pošle defaultní a proběhne registrace
(f) průběžně ukládá výsledky do ukládacího souboru, aby se neztratily v případě havárie
(g) způsob výpočtu:

- prvotní průzkum čísla algoritmem Rabin-Miller
- pokud číslo projde, bude se jeho prvočíselnost ověřovat úplně (podrobný algoritmus bude součástí zkoumání)

Návrh struktury programu

Server:
- php skript (hlavní část + pomocné funkce)
- MySQL databáze

Klient:
- hlavní program
- konfigurační a ukládací soubor (pro ukládání průběžných výsledků)

OS, jazyk, vývojové prostředí, další využívané zdroje

OS:	SuSE 10.0, Slackware 10.1
Jazyk:	PHP, C, MySQL
Vývojové prostředí:	Vim, Emacs, Anjuta, GCC, Gdb
Další využívané zdroje:	MySQL databáze, HTTP server, PHP moduly pro MySQL